INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

PERSONAL DATA RIGHTS, DEEPFAKE ADVERTISING AND THE RIGHT TO PRIVACY: A LEGAL ANALYSIS

AUTHORED BY - SUVARNA. U

Abstract

Advertising has entered an era in which a consumer's own biometric identity — face, voice and mannerism — can be synthesised without her knowledge and deployed to sell a product she has never used. This paper studies the intersection of personal data protection law and deepfake-enabled advertising in India, and the resulting strain on the constitutional right to privacy recognised in Article 21. The paper traces the evolution of India's data protection regime from the Information Technology Act, 2000 to the Digital Personal Data Protection Act, 2023 and the 2025-26 amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which for the first time define and regulate "synthetically generated information". It examines the judicial development of personality and publicity rights through cases such as Anil Kapoor v Simply Life India, Amitabh Bachchan v Rajat Nagi and the Sadhguru deepfake litigation, and situates these developments against the constitutional privacy jurisprudence of Justice K S Puttaswamy v Union of India and R Rajagopal v State of Tamil Nadu. The paper argues that although India now has a labelling and takedown framework for synthetic content, a structural gap remains between data protection law, which regulates "personal data", and personality-rights law, which protects likeness and voice, leaving deepfake advertising inadequately addressed by either regime standing alone. The paper concludes with suggestions for a converged framework of consent, labelling, and rapid redress.

Keywords

Deepfake, Personal Data, Right to Privacy, Personality Rights, Digital Personal Data Protection Act 2023, Synthetically Generated Information, Article 21, Consumer Protection, Advertising, Artificial Intelligence

ISSN: 2582-6433

1. Introduction

Advertising has always traded on persuasion, but the arrival of generative artificial intelligence has altered the terms of that trade. A "deepfake" is synthetic audio-visual media generated or altered by artificial intelligence so that a person appears to say or do something she never said or did[1]. What began as a novelty in entertainment and satire has migrated into commerce: synthetic voices and faces of film stars, singers and ordinary consumers are now used, often without consent, to manufacture false endorsements, fabricated testimonials and fraudulent investment pitches[2]. Because a synthetic advertisement of this kind depends entirely on the extraction and manipulation of a real person's biometric and behavioural data, it sits at the confluence of two distinct legal regimes: the law of personal data protection, and the law of privacy and personality.

India's constitutional foundation for both regimes is Article 21 of the Constitution, under which the Supreme Court in *Justice K S Puttaswamy (Retd) v Union of India* recognised privacy, including informational privacy, as an intrinsic part of the right to life and personal liberty[3]. That judgment catalysed the enactment of the Digital Personal Data Protection Act, 2023, India's first comprehensive data protection statute[4], and, more recently, prompted the Government to amend the intermediary rules to specifically address synthetic media[5]. Parallel to this statutory development, the Delhi High Court has, through a series of interim orders, fashioned a common-law right of personality that protects a person's name, voice, image and likeness against unauthorised commercial exploitation, including through AI tools[6].

This paper examines whether these two strands of law — data protection on the one hand, and privacy/personality jurisprudence on the other — adequately address the specific harm of deepfake advertising, in which a person's data is not merely collected or processed, but

[1]"Synthetically generated information" is now a defined statutory term under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, as amended, meaning information that is artificially or algorithmically created, generated, modified or altered using a computer resource in a manner that appears reasonably authentic or true. See Ministry of Electronics and Information Technology, Explanatory Note on the draft amendments to the IT Rules 2021 (22 October 2025).
[2]Over 120,000 AI-generated deepfakes are estimated to emerge in India every month; see NASSCOM, cited in PMF IAS, 'IT Amendment Rules, 2025: Significance and Challenges' (2025).
[3]Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (Supreme Court of India).
[4]Digital Personal Data Protection Act 2023 (No 22 of 2023).
[5]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025/2026, amending the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
[6]Anil Kapoor v Simply Life India & Ors, CS(COMM) 652/2023 (Delhi High Court, interim order dated 20 September 2023).

ISSN: 2582-6433

resynthesised into a false commercial performance. The paper proceeds in six further parts: conceptual foundations, the legal framework, the anatomy of deepfake advertising, judicial developments, an analysis of major legal issues, and findings, before offering suggestions for reform.

2. Conceptual Framework: Personal Data, Deepfakes and Privacy

2.1 Personal Data and the Data Principal

The Digital Personal Data Protection Act, 2023 defines "personal data" broadly as any data about an individual who is identifiable by or in relation to such data, and treats all personal data uniformly without a heightened category for "sensitive" data[7]. A person's face, voice, gait and speech patterns — the very raw material of a deepfake — are personal data in this sense, since they identify the individual. The Act, however, applies only to digital personal data, that is, data collected in digital form or subsequently digitised, and excludes personal data that has been made publicly available[8]. This publicly-available-data exclusion is significant for deepfakes: much of the raw footage used to train a synthetic model of a celebrity or public figure is drawn from publicly posted interviews, films or social media content, potentially placing the initial scraping of that data outside the Act's protective scope even though its downstream synthetic use causes serious harm.

2.2 Deepfakes and Synthetically Generated Information

Until October 2025, Indian law contained no statutory definition of a deepfake. The amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced the term "synthetically generated information" (SGI), defined as information that is artificially or algorithmically created, generated, modified or altered using a computer resource in a manner that appears reasonably authentic or true[9]. This is India's first legislative definition of synthetic content and is comparable to the European Union's approach under Article 50 of the EU Artificial Intelligence Act, which requires deployers of AI systems generating deepfakes to disclose that the content has been artificially generated or

[7]Digital Personal Data Protection Act 2023 (No 22 of 2023), s 2(t); see also Future of Privacy Forum, 'The Digital Personal Data Protection Act of India, Explained' (FPF, 2023).
[8]Digital Personal Data Protection Act 2023 (No 22 of 2023), s 3; DLA Piper, 'Data Protection Laws in India' (Data Protection Laws of the World, 2025).
[9]New rule 2(1) (wa), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, inserted by the 2025 Amendment; see Law.asia, 'India Tightens Rules on Deepfakes and AI-Generated Content' (2026).

ISSN: 2582-6433

manipulated[10]. The Rules further clarify that any reference to "information" in the unlawful-content and due-diligence provisions of the IT Rules shall be read to include synthetically generated information, closing an earlier jurisdictional gap in which platforms argued that deepfakes fell outside the scope of ordinary content-takedown obligations[11].

2.3 Right to Privacy as the Constitutional Anchor

Privacy in Indian constitutional law has both a decisional and an informational dimension. In *R Rajagopal v State of Tamil Nadu*, the Supreme Court recognised a right to control the commercial use of one's name and identity as an incident of the right to privacy[12]. This was substantially expanded in *Puttaswamy*, where a nine-judge bench held that informational privacy — the ability of an individual to control the flow of information about herself — is a facet of the right to life and personal liberty under Article 21[13]. Deepfake advertising implicates both dimensions simultaneously: it appropriates informational data about a person's face and voice, and it also imposes a decisional harm by placing words and endorsements in that person's mouth that she never chose to make, thereby distorting her public identity without her consent.

3. Legal Framework Governing Data Protection and Deepfake Content in India

3.1 The Information Technology Act, 2000

Before the enactment of a dedicated data protection statute, the Information Technology Act, 2000 provided the only, and limited, statutory basis for data protection in India, through section 43A, which imposed compensation liability on a body corporate for negligent handling of sensitive personal data, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[14]. The Act also criminalises the capturing, publishing or transmitting of images of a person's private parts without consent under section 66E, and the publication of sexually explicit material in electronic form under section 67A[15]. These provisions were drafted before generative AI existed, and their reliance on words such as "capturing" and "transmitting" assumes an underlying real image or event; where a deepfake is wholly synthetic and no genuine image

[10]Regulation (EU) 2024/1689 (Artificial Intelligence Act), art 50.
[11]New rule 3(1A), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
[12]R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632 (Supreme Court of India).
[13]Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[14]Information Technology Act 2000, s 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[15]Information Technology Act 2000, ss 66E and 67A.

ISSN: 2582-6433

was ever captured, defendants have argued that such content falls outside the literal scope of these offences, an argument that has found some traction in obscenity-law defences framing synthetic sexual content as "artistic fantasy" rather than exploitation of a real person[16].

3.2 The Digital Personal Data Protection Act, 2023

The DPDP Act establishes obligations for "Data Fiduciaries" who determine the purpose and means of processing personal data, and correlative rights for "Data Principals"[17]. Processing of personal data requires either free, specific, informed, unconditional and unambiguous consent, or falls within one of the statutorily defined "legitimate uses"[18]. The Act was notified in the Official Gazette on 11 August 2023 and is being brought into force in a phased manner: the Data Protection Board of India was constituted with effect from 13 November 2025, while the substantive compliance obligations on data fiduciaries take effect only from 13 May 2027[19]. For deepfake advertising, two features of the Act are especially consequential. First, the harvesting of a person's face or voice to train a generative model constitutes "processing" of personal data and, absent consent or a legitimate use, is unlawful under the Act; the Act's grievance and penalty mechanisms could in principle be invoked against a data fiduciary who trains a model on a person's biometric data without authorisation. Second, and more problematically, the Act regulates the collection and processing of personal data, not the downstream act of synthesis or publication of a fabricated advertisement — a gap that leaves the output of a deepfake largely outside the Act's own enforcement architecture and dependent instead on the IT Rules and personality-rights litigation discussed below.

3.3 The 2025-26 Amendments to the IT Rules: Regulating Synthetic Content

The Ministry of Electronics and Information Technology notified amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 addressing synthetically generated information, with the amendment coming into force on 15 November 2025 and further changes taking effect from 20 February 2026[20]. The amended Rules impose several obligations. Tool providers that enable the creation of synthetic content

[16]The Legal Journal on Technology, 'Deepfakes and Dignity — Why Indian Laws Need Reform Against Non-Consensual AI-Generated Content Beyond Section 67A' (2026).
[17]Digital Personal Data Protection Act 2023 (No 22 of 2023), s 2(i) and 2(j).
[18]Digital Personal Data Protection Act 2023 (No 22 of 2023), ss 6-7; Carnegie Endowment for International Peace, 'Understanding India's New Data Protection Law' (2023).
[19]Digital Personal Data Protection Rules 2025, notified 13 November 2025; DLA Piper, 'Data Protection Laws in India' (2025).
[20]Freshfields, 'India Targets Deepfakes and AI-Generated Content: Key Changes under MeitY's 2026 Amendments to the IT Rules' (2026).

ISSN: 2582-6433

must mark outputs prior to release to the user and embed metadata or a unique identifier enabling traceability[21]. Significant Social Media Intermediaries with five million or more registered users in India must obtain a declaration from users as to whether uploaded content is synthetically generated, and must deploy reasonable and proportionate technical measures to verify such declarations[22]. Where content is confirmed to be synthetic, it must be clearly and prominently labelled, with visual labels for images and video and audio disclosures for audio content; the labels and any embedded metadata may not be removed or modified by intermediaries or end users[23]. Significantly, the removal of confirmed synthetic content no longer depends on a court order or a notification from a government agency: intermediaries must remove it using reasonable efforts, failing which they risk losing the safe-harbour protection against third-party liability ordinarily available under section 79 of the IT Act[24].

Commentators have both welcomed and criticised this framework. On one view, it is the first legislative measure anywhere to impose upstream labelling obligations directly on AI tool providers, shifting accountability from passive distribution to the point of content generation[25]. On another view, by requiring platforms to proactively identify, verify and label synthetic content, Rule 3(3) transforms intermediaries from neutral conduits into active regulators of speech, without express statutory exemptions for satire, news reporting or artistic expression, and with rule-making, enforcement and adjudicatory power concentrated in the executive[26]. Both critiques are relevant to deepfake advertising: labelling requirements are well suited to a commercial deepfake, where speech interests are comparatively weak and consumer protection interests are strong, but the same mechanism, applied without calibration, risks over-removal of legitimate parody or brand commentary.

3.4 Overlapping Criminal Provisions

The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, contains provisions on cheating by personation, forgery, and defamation that can be invoked against the creators of fraudulent deepfake advertisements, and the amended IT Rules now require that references in earlier IT Rules to the Indian Penal Code be read as references to the Bharatiya Nyaya

[21]New rule 3(3), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021; Khurana and Khurana, 'Deepfake Regulation India 2025: MeitY's Comprehensive IT Rules Amendment' (2025).
[22]SSRana, '2025 IT Rules Amendment: Regulating Synthetically Generated Information in India's AI and Privacy Landscape' (2025).
[23]Freshfields, 'India Targets Deepfakes and AI-Generated Content' (2026).
[24]Information Technology Act 2000, s 79; Law.asia, 'India Tightens Rules on Deepfakes and AI-Generated Content' (2026).
[25]Khurana and Khurana, 'Deepfake Regulation India 2025' (2025).
[26]TechPolicy.Press, 'India's New IT Rules on Deepfakes Threaten to Entrench Online Censorship' (2025).

ISSN: 2582-6433

Sanhita[27]. These general criminal provisions were not drafted with synthetic media in mind and, as with the IT Act offences discussed above, their application to deepfakes has required interpretive extension rather than being expressly provided for by the legislature.

4. Deepfake Advertising: Nature and Modus Operandi

Deepfake advertising typically takes one of three forms. The first is unauthorised celebrity endorsement, in which a recognisable public figure's face or voice is synthetically inserted into an advertisement, investment scheme or product endorsement that the individual never agreed to. Indian courts have already confronted this pattern: Bollywood actor Anil Kapoor's image and voice were used, through generative AI tools, to sell merchandise and market motivational courses under the guise of an endorsement he never gave[28]. The second form is deceptive testimonial fabrication, where an ordinary consumer's likeness — obtained from social media or a data breach — is synthesised to appear as if she is endorsing a product, exploiting the trust that peer testimonials attract. The third is financial-fraud advertising, in which a synthetic voice or video of a trusted public figure, journalist or business leader is used to promote fraudulent investment schemes; this pattern has become sufficiently prevalent in India that it was cited as a principal driver of the 2025 IT Rules amendment[29].

Each of these forms depends on the same underlying operation: the extraction of an individual's personal data (facial geometry, vocal signature, mannerisms) without consent, followed by its algorithmic resynthesis into a commercial message. This is precisely the operation that sits awkwardly between data protection law, which regulates the input, and personality-rights law, which historically has policed the output. Consumers, meanwhile, suffer a related but distinct harm: they are deceived into purchasing decisions on the strength of an endorsement that was never in fact given, implicating consumer-protection law alongside privacy and personality rights.

[27]Vaish Associates Advocates, 'Regulation of AI-Generated/Deepfake Content and Synthetically Generated Information (SGI) in India — New Rules' (2026).
[28]Anil Kapoor v Simply Life India & Ors, CS(COMM) 652/2023 (Delhi High Court, 2023); MediaNama, 'Delhi HC Restricts Unauthorised Use of Anil Kapoor's Name, Voice' (2023).
[29]Ministry of Electronics and Information Technology, Explanatory Note on the draft amendments to the IT Rules 2021 (22 October 2025).

ISSN: 2582-6433

5. Judicial Developments

5.1 The Personality Rights Line of Cases

In November 2022, the Delhi High Court granted actor Amitabh Bachchan an ex-parte, in rem injunction restraining the unauthorised commercial use of his name, image, voice and other personality attributes — the first "John Doe" order of its kind in India for personality rights[30]. The Delhi High Court extended this reasoning in *Anil Kapoor v Simply Life India & Ors*, where sixteen defendants had used generative AI to create deepfakes of the actor, including morphing his image onto other performers and cartoon characters, generating false endorsements and motivational-course advertisements, and producing pornographic content using his likeness. Justice Prathiba M Singh held that the court could not "turn a blind eye" to such misuse, and that dilution and tarnishment of a celebrity's persona are actionable torts; the court granted an omnibus injunction restraining all defendants and unknown third parties from using the actor's name, voice, image or likeness for commercial gain, and directed domain registrars to take down infringing websites[31]. The court expressly reasoned that the celebrity also enjoys a right to privacy and does not wish his image or voice to be portrayed in contexts of his choosing, connecting personality rights doctrinally to the informational-privacy strand of Article 21[32]. The court relied on both *R Rajagopal* for the constitutional privacy dimension and on the American case *Vanna White v Samsung Electronics America* for the proposition that unauthorised commercial replication of a person's identity, even without using her actual name or image, can amount to misappropriation[33].

5.2 Extension to Other Public Figures

Similar relief has since been granted to other public figures whose voices or images were exploited by AI tools without consent, including singer Arijit Singh, whose interim relief against unauthorised AI voice-cloning platforms was granted by the Bombay High Court, and spiritual leader Sadhguru Jagadish Vasudev, whose case before the Delhi High Court in 2025 was cited by the Government as part of the impetus for the IT Rules amendments on synthetic

[30]Amitabh Bachchan v Rajat Nagi & Ors, CS(COMM) 819/2022 (Delhi High Court, interim order dated 25 November 2022); Naik Naik, 'Delhi HC's Protection to Anil Kapoor; A Landmark Order on Personality Rights' (2023).
[31]Anil Kapoor v Simply Life India & Ors, CS(COMM) 652/2023 (Delhi High Court, 2023); Decrypt, "'Not Only Me': Actor Anil Kapoor Wins AI Deepfake Court Case" (2023).
[32]LiveLaw, 'Delhi High Court Protects Actor Anil Kapoor's Personality Rights, Restrains Misuse of His Name, Image or Voice Without Consent' (2023).
[33]R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632; Vanna White v Samsung Electronics America Inc 971 F 2d 1395 (9th Cir 1992); Khurana and Khurana, 'Understanding the Relevance of the Anil Kapoor vs Simply Life India & Ors Case' (2025).

ISSN: 2582-6433

content[34]. Taken together, this body of interim orders indicates that Indian courts are willing to treat AI-enabled misuse of a person's persona as an actionable violation of privacy and personality rights independent of, and often faster than, statutory remedies, though these remedies remain case-specific, injunctive, and dependent on a plaintiff with the resources to litigate — a limitation of little assistance to the ordinary consumer whose image is misappropriated for a fabricated testimonial.

5.3 The Constitutional Privacy Foundation

The doctrinal bridge between these commercial-law outcomes and constitutional privacy law remains *Puttaswamy*, which held that any invasion of privacy by the State must satisfy the tests of legality, legitimate aim and proportionality, and that informational self-determination — the individual's ability to control data about herself — is integral to dignity under Article 21[35]. While *Puttaswamy* concerned State action, its reasoning on informational autonomy has been extended by subsequent statutory and judicial development to horizontal relationships between private parties, informing both the DPDP Act's consent architecture and the personality-rights reasoning in the Bachchan and Kapoor line of cases.

6. Analysis of Major Legal Issues

6.1 The Data Protection / Personality Rights Gap

The central structural problem identified by this paper is that the DPDP Act and the personality-rights doctrine developed by the Delhi High Court operate on different conceptual objects. The DPDP Act protects "personal data" — discrete informational inputs — and vests enforcement in the Data Protection Board, a body still in the early stages of institutional operation and with substantive obligations not fully in force until May 2027[36]. Personality-rights doctrine, by contrast, protects the synthesised output — the persona as ultimately presented to the public — but exists only as case law developed through interim injunctions, without a codified cause of action, statutory damages framework or clear standard for who may claim such a right beyond established celebrities. A deepfake advertisement is simultaneously an unlawful processing of personal data and an unlawful exploitation of persona, yet a victim must currently choose between two incomplete remedies rather than invoking a single, integrated one.

[34]SSRana, '2025 IT Rules Amendment: Regulating Synthetically Generated Information in India's AI and Privacy Landscape' (2025).
[35]Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[36]DLA Piper, 'Data Protection Laws in India' (2025).

ISSN: 2582-6433

6.2 Consent, Publicly Available Data and the Training-Data Problem

Because the DPDP Act's protective scope does not extend to personal data that has been made publicly available, and because much of the training data used to build generative models of real people is scraped from publicly accessible photographs, interviews and social media posts, a significant portion of the deepfake supply chain arguably falls outside the Act's consent requirements altogether. This mirrors a global regulatory gap: the European Union's GDPR similarly struggles to characterise the scraping of publicly posted images for AI training as "processing" requiring a lawful basis, while the EU AI Act instead imposes downstream transparency obligations on the resulting synthetic output rather than upstream restrictions on data collection[37]. India's 2025-26 IT Rules amendments adopt a broadly similar strategy, regulating the labelling of synthetic output rather than the lawfulness of the underlying data collection, which leaves the initial appropriation of a person's biometric likeness comparatively under-regulated.

6.3 Intermediary Liability and the Safe Harbour

The removal of the requirement for a court order or government notification before a significant social media intermediary must take down confirmed synthetic content is a meaningful shift in the balance of intermediary liability under Indian law, and directly benefits victims of deepfake advertising by shortening the time between detection and removal[38]. However, independent detection accuracy for AI-generated content remains limited, with commentators estimating current detection tools achieve only 65 to 70 per cent accuracy, which constrains the practical reliability of platform self-verification obligations and creates a risk of both under- and over-enforcement[39]. For deepfake advertising specifically, where the harm is commercial deception rather than political speech, the calibration challenge is somewhat easier than in the political-speech context, since courts and platforms can draw on existing advertising and trademark law standards of consumer confusion to supplement the newly labelled synthetic-content regime.

6.4 Comparative Perspective

India's approach — statutory labelling and traceability obligations on tool providers and platforms, combined with judicially developed personality rights — differs from the two principal comparative models. The European Union's AI Act imposes a harmonised, risk-based

[37]Regulation (EU) 2016/679 (General Data Protection Regulation); Regulation (EU) 2024/1689 (Artificial Intelligence Act), art 50.
[38]Law.asia, 'India Tightens Rules on Deepfakes and AI-Generated Content' (2026).
[39]PMF IAS, 'IT Amendment Rules, 2025: Significance and Challenges' (2025).

ISSN: 2582-6433

transparency obligation applicable across all twenty-seven member states, with a compliance deadline of August 2026 for deepfake-marking obligations[40], while the United States has proceeded narrowly and reactively, with the federal TAKE IT DOWN Act of 2025 focused specifically on non-consensual intimate imagery rather than deepfake advertising or endorsement fraud more broadly[41]. China's September 2025 regulation on identifying AI-generated synthetic content similarly requires clear labelling by platforms and voluntary disclosure by users, and further obliges app distributors to verify that AI applications embed identification tools before distribution[42]. India's framework sits closest to the EU model in adopting a statutory definition and labelling mandate, but currently lacks the EU's risk-tiered structure and instead relies on judge-made personality rights to fill the gap left by generalised labelling requirements — an arrangement that is flexible but, as noted above, uneven in its accessibility to non-celebrity claimants.

7. Findings and Discussion

This study finds, first, that India's data protection and intermediary-regulation framework has moved rapidly since 2023 from having no specific reference to synthetic media to possessing one of the more detailed statutory labelling and traceability regimes globally, but that this framework was designed primarily to address misinformation, electoral integrity and non-consensual intimate imagery, and only incidentally addresses commercial deepfake advertising and endorsement fraud.

Second, the judicially developed personality-rights doctrine, while doctrinally connected to Article 21 privacy jurisprudence, remains an ad hoc, injunction-based remedy accessible in practice mainly to well-resourced celebrities and public figures, rather than a codified right available to the ordinary consumer whose photograph or voice is misappropriated for a fabricated testimonial.

Third, the DPDP Act's exclusion of publicly available personal data from its protective scope, combined with the phased and still-incomplete coming into force of its substantive obligations,

[40]Regulation (EU) 2024/1689 (Artificial Intelligence Act), art 50; ddg.fr, 'A Landmark Case in India on AI Generated Avatars' (2024).
[41]Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act 2025 (US); Tech Policy. Press, 'India's New IT Rules on Deepfakes Threaten to Entrench Online Censorship' (2025).
[42]SSRana, '2025 IT Rules Amendment: Regulating Synthetically Generated Information in India's AI and Privacy Landscape' (2025).

ISSN: 2582-6433

means that the statute most naturally suited to regulating the unauthorised extraction of biometric data for deepfake training will not be fully operative until May 2027, leaving a multi-year period in which the IT Rules' labelling regime and judicial personality rights must bear the principal regulatory weight.

Fourth, none of the presently applicable frameworks squarely addresses the consumer-protection dimension of deepfake advertising — the deception of the purchasing public — leaving that dimension to be addressed, if at all, through general consumer protection and advertising-standards law rather than through privacy or data protection law specifically.

8. Suggestions

8.1 A Statutory Right of Publicity Linked to Data Protection

Parliament should consider codifying a statutory right of publicity or personality, defining unauthorised commercial synthesis of a person's name, voice, image or likeness as a form of unlawful processing of personal data under the DPDP Act, thereby allowing a single complaint to the Data Protection Board to address both the informational and reputational dimensions of a deepfake advertisement, rather than requiring separate proceedings before civil courts and the Board.

8.2 Extending Protection to Non-Celebrity Consumers

The labelling and takedown obligations introduced by the 2025-26 IT Rules amendments should be paired with a simplified, low-cost grievance mechanism specifically for ordinary individuals whose likeness is used in a fabricated advertisement or testimonial, given that the existing personality-rights remedy through civil injunction is realistically available only to claimants with the resources to litigate.

8.3 Regulating the Training-Data Stage

The publicly-available-data exclusion under the DPDP Act should be reconsidered specifically in the context of AI model training, so that the mass scraping of a person's publicly posted photographs or videos for the purpose of building a generative likeness model requires either consent or falls within a narrowly defined legitimate use, consistent with the direction taken by the EU AI Act's transparency obligations for deepfake generation.

ISSN: 2582-6433

8.4 Advertising-Specific Verification Standards

Sector regulators such as the Advertising Standards Council of India should be empowered to require pre-publication verification of celebrity or influencer endorsements against a registry of authorised endorsement contracts, so that a synthetic endorsement can be more easily distinguished from a genuine one at the point of publication rather than only after a complaint or litigation.

8.5 Accelerated Implementation Timeline

Given the pace at which generative AI tools are being deployed for commercial deception, the Government should consider accelerating the phased implementation of the DPDP Act's substantive compliance obligations, at least for significant data fiduciaries whose services are demonstrably used to create or distribute synthetic commercial content, rather than deferring full implementation to May 2027 uniformly across all sectors.

Conclusion

Deepfake advertising exposes a seam between two branches of Indian law that developed largely independently of one another: data protection law, concerned with the lawful collection and processing of personal information, and personality-rights jurisprudence, concerned with the unauthorised commercial exploitation of an individual's identity. Both branches trace their constitutional lineage to the right to privacy recognised in *Puttaswamy*, and both have been substantially strengthened in the past three years — the DPDP Act through its enactment and phased implementation, and personality rights through the Delhi High Court's Bachchan and Kapoor line of orders, now reinforced by a statutory labelling and traceability regime for synthetically generated information under the amended IT Rules. Yet a synthetic advertisement built from a person's stolen likeness continues to fall between these regimes rather than squarely within either. A more coherent framework — one that treats the unauthorised synthesis of a person's identity for commercial gain as, simultaneously, an unlawful processing of personal data and a violation of the right to privacy — remains the most important reform needed in this area of law.

ISSN: 2582-6433

References

Primary Sources

Legislation

Constitution of India 1950, arts 19, 21, 300A.

Information Technology Act 2000.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025/2026.

Digital Personal Data Protection Act 2023 (No 22 of 2023).

Digital Personal Data Protection Rules 2025.

Bharatiya Nyaya Sanhita 2023.

Regulation (EU) 2016/679 (General Data Protection Regulation).

Regulation (EU) 2024/1689 (Artificial Intelligence Act).

Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act 2025 (US).

Cases

Amitabh Bachchan v Rajat Nagi & Ors, CS(COMM) 819/2022 (Delhi High Court).

Anil Kapoor v Simply Life India & Ors, CS(COMM) 652/2023 (Delhi High Court).

Justice K S Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (Supreme Court of India).

R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632 (Supreme Court of India).

Sadhguru Jagadish Vasudev & Anr v Unknown Defendants (Delhi High Court, 2025).

Vanna White v Samsung Electronics America Inc 971 F 2d 1395 (9th Cir 1992) (United States).

Secondary Sources

Articles, Reports and Online Sources

Carnegie Endowment for International Peace, 'Understanding India's New Data Protection Law' (2023) <carnegieendowment.org>.

ddg.fr, 'A Landmark Case in India on AI Generated Avatars' (2024) <www.ddg.fr>.

Decrypt, '"Not Only Me': Actor Anil Kapoor Wins AI Deepfake Court Case" (2023) <decrypt.co>.

DLA Piper, 'Data Protection Laws in India' (Data Protection Laws of the World, 2025)

ISSN: 2582-6433

<dlapiperdataprotection.com>.

Freshfields, 'India Targets Deepfakes and AI-Generated Content: Key Changes under MeitY's 2026 Amendments to the IT Rules' (2026) <freshfields.com>.

Future of Privacy Forum, 'The Digital Personal Data Protection Act of India, Explained' (2023) <fpf.org>.

Khurana and Khurana, 'Deepfake Regulation India 2025: MeitY's Comprehensive IT Rules Amendment' (2025) <khuranaandkhurana.com>.

Khurana and Khurana, 'Understanding the Relevance of the Anil Kapoor vs Simply Life India & Ors Case' (2025) <khuranaandkhurana.com>.

Law.asia, 'India Tightens Rules on Deepfakes and AI-Generated Content' (2026) <law.asia>.

LiveLaw, 'Delhi High Court Protects Actor Anil Kapoor's Personality Rights, Restrains Misuse of His Name, Image or Voice Without Consent' (2023) <livelaw.in>.

MediaNama, 'Delhi HC Restricts Unauthorised Use of Anil Kapoor's Name, Voice' (2023) <medianama.com>.

Ministry of Electronics and Information Technology, Explanatory Note on the draft amendments to the Information Technology Rules 2021 (22 October 2025) <meity.gov.in>.

Naik Naik, "Delhi HC's Protection to Anil Kapoor; A Landmark Order on Personality Rights" (2023) <naiknaik.com>.

PMF IAS, 'IT Amendment Rules, 2025: Significance and Challenges' (2025) <pmfias.com>.

SSRana, '2025 IT Rules Amendment: Regulating Synthetically Generated Information in India's AI and Privacy Landscape' (2025) <ssrana.in>.

TechPolicy.Press, "India's New IT Rules on Deepfakes Threaten to Entrench Online Censorship" (2025) <techpolicy.press>.

The Legal Journal on Technology, 'Deepfakes and Dignity — Why Indian Laws Need Reform Against Non-Consensual AI-Generated Content Beyond Section 67A' (2026) <thelegaljournalontechnology.com>.

Vaish Associates Advocates, 'Regulation of AI-Generated/Deepfake Content and Synthetically Generated Information (SGI) in India — New Rules' (2026) <vaishlaw.com>.