



This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Digital Personhood and the Right not to be Simulated: A Constitutional Response to AI Identity Replication

Ujjwal Kumar^a

^aSymbiosis Law School, Nagpur, India

Received 11 June 2026; Accepted 11 July 2026; Published 14 July 2026

In the digital world, human identity has drastically changed thanks to the quick growth of AI technologies like generative artificial intelligence. Today, AI-powered tools can simulate an individual's voice, face, gestures, and even thought processes with a level of detail that goes beyond deepfakes to complete personality cloning. The article reviews the current state of the law on the right to privacy in Article 21 of the Constitution of India, personality rights, and digital personal data protection under the Digital Personal Data Protection Act 2023, the Information Technology Act 2000, and copyright, and how they fall short of addressing the various harms caused by AI-generated simulation of the human identity. In light of parallels drawn from the United States, the European Union and China, the article calls for the recognition of a separate constitutional and statutory “right not to be simulated” that is based on the principles of human dignity, informational self-determination and personal autonomy in Article 21. The proposed right would give every individual a right to “withhold consent” for the replication of their identity through AI, including for commercial purposes or posthumously. The article also calls for specific legislative changes such as amendment of the Digital Personal Data Protection Act 2023, introduction of a special law on AI identity protection and creation of a separate AI regulatory body. This article thus adds to an emerging debate on digital personhood and the constitution of technological simulation.

Keywords: *artificial intelligence, right to privacy, personality rights, digital personhood, human simulation.*

INTRODUCTION

With the advent of generative Artificial Intelligence, the line between real and simulated reality is more blurred than ever. The dawn of synthetic media, also known as 'deepfakes', has made it possible to digitally alter audio-visual material so that it appears victims are saying or doing something they don't. But today, the path of AI has shifted beyond videos that have been manipulated. Complex models can now produce synthetic copies of humans with voice, facial features, emotional expression, behavioural traits and even simulated memory- what you might think is a good description of 'AI human simulation.'

The various legal, ethical, and constitutional issues within which this development occurs are very significant. One's identity – what he or she looks like, how he or she sounds, behaves, and feels – is one of the most personal of attributes. If AI systems can simulate this identity without the individual's knowledge or consent, basic questions emerge regarding autonomy, dignity, and technological innovation that is allowable.

Research Problem: India's current legal system is not built to address the issues of AI-generated human simulation. The Supreme Court's landmark decision in Justice KS Puttaswamy v Union of India revealed that privacy is a fundamental right, but the scope and definition of this right are yet to be thoroughly explored in relation to digital identity replication. Personality rights have been recognised in a series of Delhi High Court judgements but have been limited to celebrities and do not fully extend to an ordinary person to protect them from having their identity appropriated through simulation.¹

Although the Digital Personal Data Protection Act 2023 is an important piece of legislation, it is somewhat limited in scope in relation to the processing of personal data and does not regulate the processing of personal data in order to create synthetic human replicas. In the same way, section 66E of the Information Technology Act 2000 covers only intimate images and doesn't offer any remedy for wider personality simulation. The lack is a key gap in India's digital rights matrix.²³

¹ *Justice KS Puttaswamy (Retd) v Union of India & Anr* (2017) 10 SCC 1

² Information Technology Act 2000, s 66E

³ Digital Personal Data Protection Act 2023

RESEARCH QUESTIONS

This article aims to answer the following research questions:

1. What are the existing legal and constitutional lacunae in dealing with human simulation using AI?
2. Would there be a constitutional basis in dignity, autonomy and privacy under Article 21 for the recognition of a right not to be simulated?
3. What can be learned from the regulatory practices in the United States, the EU and China?
4. What changes in laws and institutions are needed to make such a right a reality in India?

OBJECTIVES OF THE STUDY

This article aims to:

- (a) chart the doctrinal lacunae in India's legal response to AI simulation;
- (b) develop a constitutional justification for the right not to be simulated under Article 21 of the Indian Constitution;
- (c) suggest a coherent statutory framework of its protection; and
- (d) make some contributions to the jurisprudence in a comparative context, concerning digital personhood and AI governance.

RESEARCH METHODOLOGY

The methodological approach of this article is doctrinal/comparative. It examines the constitutional provisions, judicial decisions, statutory instruments and legislative proposals from India and selected foreign jurisdictions. Supreme Court and High Court decisions, parliamentary committee reports and regulatory guidelines are examples of primary sources. Academic scholarship, policy papers and reports by international organisations are secondary sources.

SCOPE AND LIMITATIONS

The article has been exclusively about the identity simulation of living persons in India as compared to the United States, Europe and China, using AI. Not focused on the criminalisation of intimate imagery that has not been consented to separately, and it doesn't explore AI-generated fictional characters without real people. Only the civil/civil rights and constitutional aspects of what is proposed as a right are analysed, although criminal liability is mentioned when appropriate.

UNDERSTANDING AI-DRIVEN HUMAN SIMULATION

Development of Generative AI Technologies: Generative AI is a category of artificial intelligence models that can generate new content, such as textual, visual, auditory and visual media, based on patterns recognised from vast amounts of data. With the advent of Generative Adversarial Networks (GANs), diffusion models, and large language models (LLMs), the potential for producing synthetic media has grown exponentially, both in terms of the variety of content and its authenticity.

At first, AI-generated content used to be confined to stylistic interpolation and enhancing photos. In the mid-2010s, face-swapping algorithms emerged, leading to the creation of deepfakes that allow the attaching of one face onto another in videos. But the combination of voice cloning, behavioural modelling and multimodal AI systems has created the technology to create detailed simulations of actual individuals.

Deepfakes to Personality Replication: Replication of personae is a qualitative leap from deepfake. Deepfakes are usually generated by altering audio-visual material; however, personality replication is the creation of an independent synthetic agent modelled on a person's speech patterns, emotional reactions, tendency to make decisions, and interpersonal style.⁴

This is thanks to the availability of huge amounts of publicly available personal data – social media posts, recorded speeches, interview footage, and correspondence – that AI systems can process and use to build detailed behavioural models. The outcome is a computer-

⁴ Hao Li et al., 'Advancing High Fidelity Identity Swapping for Forgery Detection' (Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA, 2020)

generated character that can interact in real-time in the same way as the original person. In human simulation, the voice, appearance, behaviour and memory are the four components.

Components of Human Simulation: Voice, Appearance, Behaviour and Memory: There are 4 major parts of AI human simulation. Voice cloning: Voice cloning systems, like neural text-to-speech models, can mimic an individual's vocal style, pitch, and tone from very few voice samples. Second, facial simulation: photorealistic face generation models can create a visual likeness that is indistinguishable from a real photograph or video. Third, behavioural modelling: AI systems can learn from an individual's digital footprint and anticipate and simulate their style of speech, opinions and decision-making. Fourth, simulated memory: some AI persona systems are built with an artificial history of an 'individual' purported experiences and relationships, to allow contextually appropriate interactions over time.

New AI Human Replicas Use Cases: Human replicas powered by AI are used in a wide variety of applications, which continue to grow. Digital resurrection of deceased celebrities and synthetic stunt doubles are becoming more and more commonplace in the entertainment world. AI companions are being sold in the healthcare industry as tools to help people cope with grief after they've lost a loved one. Celebrity likeness is used commercially for targeted advertising, where there are no meaningful systems of consent. In the realm of politics, the synthetic copies of politicians/workers can be deployed to manufacture disinformation on a large scale.

Legal and Ethical Dangers Associated with Human Simulation: The potential legal and ethical dangers of unchecked AI human simulations are compounded. On an individual level, simulation without consent is a serious infringement of personal autonomy and dignity, and can result in reputational injury, financial fraud, intimate images without consent and psychological injury. Societally, the spread of AI reproductions poses a risk of breach of the integrity of knowledge, democratic discourse, and interpersonal trust. The marketplace of simulated identities has brought up unanswered issues of property, consent and equitable reward, which are not properly answered by current IP systems.⁵

⁵ Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review
<https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship> accessed 10 June 2026

GAPS IN INDIA'S EXISTING LEGAL FRAMEWORK

Right to Privacy under Article 21: Justice KS Puttaswamy v Union of India (2017) was a unanimous ruling of the Supreme Court of India that set the precedent for the recognition of privacy as a fundamental right in the Indian Constitution. The nine-judge bench held that the right to privacy is not a separate right but part of the right to life and personal liberty guaranteed under Article 21, which includes privacy of information, decisional privacy and body integrity. Chandrachud J spoke of privacy as the shield of the 'intimate zone' of individual existence against the incursion of the State and others.⁶

The Puttaswamy framework, however, is expansive in nature, and does not focus in particular on the phenomenon of identity simulation by means of AI. Indian constitutional jurisprudence is yet to be well-developed on the privacy aspects of simulations, especially the idea of creating synthetic profiles from publicly available information. Also, the non-existence of horizontal application doctrine in privacy law hampers the efficacy of Article 21 vis-à-vis private technology players.

Personality Rights in Indian Jurisprudence: The law of personality rights in India has been gradually built up mainly by the decisions of the Delhi High Court. The court in the case of Titan Industries Ltd v Ramkumar Jewellers held that the right of publicity is part of the intellectual property which entitles the celebrity to control the commercial use of his name, likeness, voice and other distinguishing characteristics.⁷

In ICC v ICC Development (International) Ltd, the court recognised that the distinctive personality of a public figure is a property interest which can be protected. In the case of AI simulation, though, these precedents hold three important drawbacks. First, they are limited to people with a public profile. Secondly, they focus on commercial exploitation in traditional media, not simulated AI interventions. Thirdly, they do not apply to non-commercial replication, creating AI companions or grief bots analogous to private persons, for instance.⁸

Right of Publicity and Commercial Exploitation: This right to publicity, i.e., the right of an individual to the commercial value of their personality, has already been somewhat accepted

⁶ Justice K S Puttaswamy (Retd) v Union of India & Anr (2017) 10 SCC 1

⁷ Titan Industries Ltd v M/S Ramkumar Jewellers CS (OS) No 2662/2011

⁸ ICC Development (International) Ltd v Arvee Enterprises & Anr (2003) 26 PTC 245

by Indian courts but hasn't been codified under any statute. There is no specific right of publicity statute, and remedies are therefore split between tort law, the passing off doctrine, and copyright law. The problem is exacerbated in the case of an AI simulation because this kind of harm is not necessarily related to one or a few discrete acts of commercial exploitation but to the continuous functioning of a synthetic persona system.

Copyright Law and its Inadequacies: The Copyright Act, 1957 protects original literary, dramatic, musical and artistic works. The voice, look, gestures, and personality of an individual may be covered by protection, but the individual's personality itself is not a copyrightable work. Section 57 of the Copyright Act has introduced the concept of moral rights to maintain the integrity of a work after it has been assigned, but not for the protection of personal identity *per se*.⁹

In addition, AI systems often rely on publicly available data in massive amounts to create simulations, and this data might be within the 'fair use' limits in the current copyright doctrine. The development of AI models from private data does not automatically amount to a violation of an existing IP right, leaving a considerable gap.

The Digital Personal Data Protection Act (DPDP Act), 2023: The Digital Personal Data Protection Act 2023 (DPDPA) is India's most holistic legislation to date addressing personal data governance. The DPDPA lays down a consent-driven model for processing personal data, imposes duties upon data fiduciaries and allows for various sets of rights with respect to data principals such as correction, erasure, and grievance redressal.¹⁰

But the use of personal data to create AI simulations of individuals is not directly addressed by the DPDPA. The definition of 'personal data' and the consent requirements in the Act tend to be geared towards the collection and processing of the data, and not towards the use of aggregated data to create synthetic copies of people. Significantly, the Act does not bar the use of data, when lawfully obtained, for the purpose of training an AI model that emulates an identity, nor does it specifically govern the use of such models.

Information Technology Act 2000: Section 66E of the Information Technology Act 2000 makes it illegal to send, show or publish pictures depicting the private parts of a person

⁹ Copyright Act 1957, s 57

¹⁰ Digital Personal Data Protection Act 2023

without their consent, intentionally. This provision only tackles one specific aspect of non-consensual synthetic media, in this case, pornographic deepfakes, but not the wider phenomenon of personality simulation. Section 67 and Section 67A cover obscene and sexually explicit electronic messages respectively, but are also narrow in scope.¹¹

Constitutional Justification for a Right Not to be Simulated: Indian law in its present form lacks in various aspects, with three noticeable structural gaps. First, these laws were drafted before the advent of AI technologies such as generative AI, and are a product of the regulatory imagination of an earlier technological age. Second, the current systems work to respond to isolated incidents of harm and not systemically planned and implemented synthetic identity systems. Third, in Indian law too, there is no single conceptual category of ‘digital personhood’ or ‘right to control an AI-repliquee’. This equates to a regulatory landscape where AI impersonating humans is mostly free from legal restrictions.

HUMAN DIGNITY, AUTONOMY AND DIGITAL PERSONHOOD UNDER ARTICLE 21

Constitutional Protection of Dignity of Humans: Human dignity is one of the basic values of the Constitution of India. The Preamble, which guarantees the dignity of the individual, coupled with the chapter on Fundamental Rights, has always been interpreted by the Supreme Court as placing a negative and positive responsibility on the State. In *Francis Coralie Mullin v Union Territory of Delhi, Bhagwati J* pronounced that Article 21 includes the right to live with basic dignity of human beings, the right to be treated as human and not as a means to an end.¹²

Dignity's connection with AI simulation is one-step: when a person's likeness is reproduced without their consent, their identity becomes a means to an end – whether commercial, entertainment or political – and the human being themselves becomes disregarded. Such instrumentalisation is contrary to the constitutional vision of dignity and a good normative argument for limiting AI simulation.

Informational Self-Determination: In Germany, the term ‘informational self-determination’ is based on constitutional law and was transposed to various forms of law in the legal

¹¹ Information Technology Act 2000, ss 67 and 67A

¹² *Francis Coralie Mullin v The Administrator, Union Territory of Delhi & Ors* (1981) 1 SCC 608

systems of different jurisdictions, the core of which is a fundamental right to control the collection, use and dissemination of information concerning a person. In India, the Court has given its thumbs up in *Puttaswamy*, with several judges stating that the right to control personal information is part of the constitutionally guaranteed right to privacy.¹³

The idea of informational self-determination is of particular relevance for the use of AI simulation: the creation of a synthetic replica of a person inevitably requires processing of personal data voice recordings, photographs, behavioural data without the person's active, meaningful consent. If informational self-determination is considered a separate constitutional right, individuals can block the use of their own information for simulation, regardless of whether the data collection is legal or not.

Personal Autonomy in the Digital Age: The Supreme Court has identified the right to personal autonomy, that is, to make meaningful choices about one's life without undue interference from others, as one of the essential aspects of the right to life and personal liberty. In *Maneka Gandhi v Union of India*, the court had ruled that any procedure that impairs the right to life must be 'fair, just and reasonable,' which was actually an implicit incorporation of a substantive understanding of personal freedom.¹⁴

In the digital world, personal autonomy translates to control of one's digital presence and digital identity. Since an AI replica is created, speaks, and interacts in the same manner as the original individual without their consent, it undermines the individual's autonomy by separating their identity from their will. The person is a passive object of his or her own virtual life, and they cannot set the actions or images that are assigned to them in that space.

The Concept of Digital Personhood: Digital Personhood is defined as a person's whole identity, agency and relationships in the digital space. In the digital age, where individuals are more connected via social media, online transactions, digital communications, and AI interactions, safeguarding digital personhood is closely interconnected with the protection of physical personhood and human flourishing. Digital personhood is based on a philosophical tradition of personal identity as revealed through continuity of story,

¹³ *Volkszählungsurteil* [1983] BVerfGE 65; Spiros Simitis, 'REVIEWING PRIVACY IN AN INFORMATION SOCIETY' (1987) 135(3) *University of Pennsylvania Law Review* <<https://www.jstor.org/stable/3312079>> accessed 10 June 2026

¹⁴ *Maneka Gandhi v Union of India* AIR 1978 SC 597

recognition in relation to others, and expression in acts of agency. An AI replica that pretends to be a person infringes on all three aspects: imposes a story on an individual without their consent, provides relational recognition that the person didn't have, and provides agency that the person was not given.

Constitutionally Justified Right Not to be Simulated: The dignity of the individual coupled with informational self-determination, personal autonomy and digital personhood secures a strong constitutional basis for the right to not be simulated under Article 21. This right would include the entitlement of every individual to deny the ability of AI systems to replicate herself or himself for commercial, entertainment, political or personal ends and to demand effective remedies for the lack of replication in the absence of her or his specific, free and informed consent. The right does not mean an absolute right: Any constitutional right can be proportionately curtailed in the public interest. Under a well-drafted law, there may be certain law enforcement uses, as well as uses for journalistic commentary, academic research, satire and parody, which could be considered permissible reasons for simulation. The starting point, however, must be the person's presumed right to refuse simulation, and the burden to simulate must be on those who want to intrude.

GLOBAL LEGAL AND REGULATORY RESPONSES TO AI IDENTITY REPLICATION

US: Publicity & Likeness Rights: The current landscape of AI identity replication regulation in the United States is made up of a mix of state right of publicity laws, federal proposed legislation, and nascent common law doctrine. California Civil Code §3344 safeguards people from the unauthorised use of their name, voice, signature, photograph or likeness for commercial purposes.¹⁵ The proposed 'No Fakes Act 2023' would implement a federal right against creating digital copies of people's voice or physical likeness without their consent; the right would last 70 years after death. The difference lies between the use of replicas for commercial purposes and their use for news, comment or satire. The US approach is more based on property rights, and is about the more economic aspects of identity exploitation, and not about dignity or autonomy interests.¹⁶

¹⁵ California Civil Code 2023, s 3344

¹⁶ No Fakes Act 2023, s 3096

Privacy and Data Protection Approaches in the European Union (EU): The European Union's framework for replicas of AI identity is primarily through the GDPR and the EU Artificial Intelligence Act 2024. Under the GDPR, Article 22 regulates automated decision-making that is likely to produce significant effects, including legal effects, on a data subject. At the same time, the AI Act includes provisions to regulate transparency obligations and conformity assessments for certain high-risk AI systems, such as biometric and emotion recognition systems.¹⁷ The GDPR's principle of purpose limitation also applies to using personal data collected for a specific purpose for AI training, which requires obtaining new consent. Unlike the US conception of identity protection, which is based on property rights, the EU approach views AI simulation in the context of a larger vision of data protection and fundamental rights.¹⁸

China: Deep Synthesis Technologies' Regulation: The Deep Synthesis Provisions published by the Cyberspace Administration of China in 2022 are the most recent and detailed regulation of synthetic media in China. The stipulations are that any provider using such 'deep synthesis' technologies needs to get consent from those whose likeness, voice, or identity is being reproduced, and that all synthetic content must be identified as such.¹⁹ The Deep Synthesis Provisions ban the application of AI synthesis technologies if they pose a threat to national security, disturb social order, violate personal rights or disseminate false information. The Provisions apply not just to static deepfake content as in previous frameworks but to 'personality replicas', or interactive AI personas. But the regulatory regime is part of a wider surveillance system and is not a model for a liberal democratic system.

Learning for the Indian Legal System: The comparative analysis uncovers three main lessons for India. The US model illustrates the need to have a specific legislative tool in place, instead of relying on general remedies that are available under tort law or property law. Second, the EU model emphasises the importance of embedding a form of AI-simulation in a larger fundamental rights context, including dignity and autonomy as well as property interests. Third, the Chinese model shows the regulatory impact of enforcing mandatory consent procedures and labelling requirements, although the overall regulatory framework

¹⁷ General Data Protection Regulation 2016, art 22

¹⁸ Artificial Intelligence Act 2024

¹⁹ Provisions on the Administration of Deep Synthesis Internet Information Services 2022

may not be directly applicable. India's constitutional system, which has a long history of robust substantive adjudication of fundamental rights, offers a ripe setting for a combination of all three models: a special statutory bill of rights with clear consent provisions, robust enforcement provisions and proportionate exceptions.

THE CASE FOR A RIGHT NOT TO BE SIMULATED

What is the Right Not to be Simulated: This article suggests the establishment of a 'Right to Not Be Simulated' as an underlying fundamental right enshrined in Article 21 of the Constitution of India. The right is every individual's right to refuse the creation, deployment, and sharing of an AI replica or simulation of their voice, appearance, behavioural patterns, personality, etc., without their free, informed, specific and revocable consent.²⁰ The right works as a negative right (a duty) for persons and entities not to mimic an individual's identity without his or her consent, as well as a positive right for the State to provide legislative and institutional responses sufficient to realise that the negative right is made effective in practice.

Scope & Nature of the Proposed Right: About the scope of the right, the 'not to be simulated' does not just apply to those who have already been made visible online, regardless of their professional status or starring role in public online discussions. The right itself is not like the current personality rights doctrine, which only protects certain celebrities, but rather everyone has a constitutionally important interest in their identity that should be protected from simulation without their consent. This right also applies to all forms of identity simulation: visual resemblance, voice, text-based personality models, interactive AI agents and hybrid forms. It applies to any type of simulation (for profit, art, information, private) subject to the proportionate exceptions below.

Consent as the Basis for Protection: Consent is at the heart of the proposed right. Four conditions beyond which consent can no longer be legally considered to exist are: consent must be free (without coercion or influenced by the power differential typical of digital platform relationships); consent must be informed (based on clear disclosure of the nature, purpose and scope of the simulation); consent must be specific (directly connected to the

²⁰ *Justice K S Puttaswamy (Retd) v Union of India & Anr* (2017) 10 SCC 1; The Constitution of India 1950, art 21; Sujit Choudhry et al., *The Oxford Handbook of The Indian Constitution* (OUP UK 2016)

specific form of simulation proposed and not obtained through blanket terms and conditions); consent must be revocable (able to be withdrawn at any time for no detriment to the individual).²¹ The specificity requirement is especially knotty in the AI world, where people may have permitted a specific recording, such as an interview, to be used to train an AI model that can generate an unlimited number of simulated recordings. If there is a right to be non-simulated, this would prevent any mission creep and mandate new and specific consent for each additional use.²²

Protection Against Commercial Exploitation: The most readily implementable aspect of the asserted ‘right’ is the ability to use the simulated identity commercially, for advertising, entertaining, political campaigning and digital commerce. This right to non-simulation would allow individuals to sue for an injunction and damages to be awarded to those who use, without permission, simulated replicas for commercial purposes. The damages should consider the actual economic damage done to the individual and the unjust enrichment of the person who used the simulation. It would provide the right deterrent incentives, as well as limit the economic benefits of identity simulation to be distributed in a way that is not disproportionate to the technology actors.

Posthumous Protection of Identity: Emerging AI simulation technologies permit the digitisation and recreation of deceased persons, sparking specific worry about the ability for the living to manipulate images of those who have passed. The proposed right to be not simulated should be operative for a minimum of 70 years after the individual's death through representatives/successors of his choice.²³ The protection of reputation is important but becomes particularly significant in cultural, religious and political contexts where the reputation of the deceased may be abused for purposes that run counter to his or her values. Without the proper permission, the digital resuscitation of dead politicians, religious leaders

²¹ Digital Personal Data Protection Act 2023; General Data Protection Regulation 2016

²² Lilian Edwards and Michael Veale, ‘Enslaving the Algorithm: From a ‘Right to an Explanation’ to a ‘Right to Better Decisions’?’ (2018) 16(3) IEEE Security & Privacy <<https://ieeexplore.ieee.org/document/8395080>> accessed 10 June 2026; Sandra Wachter et al., ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7(2) International Data Privacy Law <<https://academic.oup.com/idpl/article-abstract/7/2/76/3860948?redirectedFrom=fulltext>> accessed 10 June 2026

²³ No Fakes Act 2023, s 3096; Cal Civ Code 2025, § 3344.1

or cultural celebrities calls into question not only their individual dignity, but collective cultural rights as well.²⁴

Civil and Regulatory Remedies: To be effective, enforcement of the right not to be simulated needs to be combined in a multi-layered remedial framework. At the civil level, punishments should include the right to an injunction against the creation or further use of unauthorised simulations, compensation for damage to reputation, psychological damage, and economic damage, and account of profits if commercial exploitation of the simulation has taken place.²⁵

The AI regulatory body outlined in section 7 should have the ability to investigate complaints, impose financial sanctions on entities and companies that deploy simulations without consent, and mandate the removal of illegitimate synthetic content. Intermediary liability rules should be modified to ensure that, when notified of a simulated image, the provider of the platform is obliged to remove it.

Balancing Innovation with Individual Rights: Recognising the right not to be simulated must also be fine-tuned so as not to hinder lawful innovation on generative AI. Under the framework of proportionality, the author proposes that sometimes simulation without consent may be acceptable if:

- (a) The simulation is about journalistic commentary, academic research or if it is a genuine satire and parody;
- (b) The simulation is necessary for law enforcement or national security purposes under judicial oversight;
- (c) The individual is a public figure, and the simulation has nothing to do with his or her private life.

These are enumerated exceptions and are limited. Commercial exploitation, entertainment, personal use, etc., is not covered by them, and the consent requirement continues to apply.

²⁴ Edina Harbinja, 'Post-mortem privacy 2.0: theory, law, and technology' (2017) 31(1) *International Review of Law, Computers and Technology* <<https://dl.acm.org/doi/10.5555/3059279.3059282>> accessed 10 June 2026

²⁵ *Titan Industries Ltd v M/S Ramkumar Jewellers* CS (OS) No 2662/2011; Roberta Rosenthal Kwall, *The Soul of Creativity* (Stanford University Press 2009)

A party that is conducting the simulation is responsible for the burden of proof on whether or not it qualifies as a permissible exception.

DESIGNING A LEGAL FRAMEWORK FOR PROTECTION AGAINST AI SIMULATION

Legislative Reforms: A standalone AI Identity Protection (IDP) Act should be enacted as the key legislative mechanism to implement the right not to be simulated. Such an Act should:

- (a) define the terms ‘AI simulation’ and ‘digital replica’ in a technologically-neutral way that accounts for future advances;
- (b) make the right not to be simulated a statutory right;
- (c) specify the conditions for valid consent;
- (d) prescribe the cases in which such a right can be excluded;
- (e) introduce civil remedies and penalties; and
- (f) include compulsory disclosure requirements for AI systems producing synthetic human content.

Amendments to Existing Laws: The Digital Personal Data Protection Act must be complemented with the following amendments:

- (a) Make it expressly prohibited to use personal data for training an AI model for simulating identities without any specific consent of data subjects;
- (b) Propose introducing the obligation for data fiduciaries to inform data subjects about how and for which purposes their personal data is being used in any AI model at the time of collection;
- (c) Make it possible to delete personal data collected for AI training models, upon specific request.

Amend the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021²⁶ to mandate platforms to:

- (a) have automated systems that detect AI-generated synthetic content featuring identifiable individuals;
- (b) adopt a speedy takedown mechanism for non-consensual simulations; and
- (c) provide an easy complaints forum for affected individuals.

AI Governance Mechanisms: There is no specific regulatory authority for AI in the existing regulatory framework of India. The article proposes the creation of an independent AI Governance Commission responsible for

- (a) monitoring compliance with AI identity protection laws,
- (b) maintaining a register of AI systems used for simulating and generating identities,
- (c) providing binding guidance on standards of consent and acceptable uses of AI systems and
- (d) periodically assessing the regulation taking into account technological advances.

Management and Enforcement Systems: The AI Governance Commission should be independent and composed of members from legal and technical, civil society and academic backgrounds. The enforcement authority should include investigation, summoning of witnesses, imposition of civil sanctions, and referring cases of criminal non-compliance to the relevant authorities.

International cooperation mechanisms need to be developed to cover the cross-border aspects of AI simulation, such as the use of simulations by entities of foreign jurisdictions. India should discuss harmonised standards for AI identity protection with international bodies such as the UN Special Rapporteur on the Right to Privacy and the OECD AI Policy Observatory.

²⁶ IT (Intermediary Guidelines) Rules 2021; *Shreya Singhal v Union of India* (2015) 5 SCC 1

KEY RECOMMENDATIONS

The article makes the following five major recommendations:

Constitutional Recognition: The Supreme Court of India, in line with the principles of human dignity, information self-determination and informational self-determination, should also recognise that there is a right not to be simulated implicit in the right to life and personal liberty conferred by Article 21 of the Indian Constitution.

Dedicated Legislation: Parliament should pass a dedicated AI Identity Protection Act that would make the right not to be simulated a right enshrined in law with the following requirements: Consent should be obtained. Exceptions must be specified. Remedies should be available and effective.

Amend the Digital Personal Data Protection Act 2023 by making a provision for barring the usage of personal data for simulation purposes through AI training without specific consent.

Independent Regulatory Authority: There must be an independent AI Governance Commission to monitor compliance, investigate complaints, and take necessary sanctions.

International Engagement: India must be actively involved in international norm-setting discussions on AI identity protection to make sure that its national regulatory developments align with evolving international norms.

CONCLUSION

This article has evidenced the inability of the current legal landscape of India, which includes the constitutional privacy framework, the personality rights jurisprudence, the Digital Personal Data Protection Act 2023, the Information Technology Act 2000, and the copyright law, to deal with the innovative and complex harms caused by AI-enabled human simulation. Generative AI technologies are evolving at an unprecedented pace, making it difficult to apply current regulatory frameworks that are structurally inadequate to address the rapidly unfolding and complex landscape of AI.

The right not to be simulated is a welcome development and an evolution of constitutional and statutory jurisprudence in the face of transformative challenges of the AI age. In the future, with the growing sophistication and accessibility of AI technologies, safeguarding

individual identity against unauthorised simulations will be a growing imperative for constitutional democracy.

The right not to be simulated cannot be a right against technology per se; it is a right to make sure technology contributes to human flourishing rather than to human harm. Such recognition would bring to full fruition the constitutional promise of dignity, autonomy, and privacy in every facet of life – digital and simulated life alike – and the idea that no technological development should be pursued if it jeopardises the ‘fundamental values’ that form the basis of the constitutional order.