International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Watching Without Warrant: Artificial Intelligence Surveillance, Behavioural Profiling and the Right to Privacy Under Article 21 of the Constitution of India

Markapuram Mahima[a]

[a]Symbiosis Law School, Hyderabad, India

Received 27 May 2026; Accepted 26 June 2026; Published 29 June 2026

The emergence of AI companion application tools that generate synthetic romantic partners, AI boyfriends, AI girlfriends, and emotionally responsive chatbots marks a qualitatively new frontier in the relationship between artificial intelligence and personal privacy. This paper examines how AI companions, generative face tools, and behavioural profiling raise serious Article 21 privacy concerns. It argues that these issues matter mainly through the State's duty to protect privacy and regulate data use, while noting that existing Indian law still leaves major gaps. When a user asks ChatGPT to "create a boyfriend/girlfriend," when Replika generates a synthetic partner from scraped photographs, or when a generative AI tool produces a photorealistic face that belongs to a real person who never consented to its use, something constitutionally significant has occurred. This paper argues that these practices, alongside the broader architecture of AI behavioural surveillance conducted by platforms such as Meta, YouTube, Instagram, and DeepSeek, raise serious concerns regarding the fundamental right to privacy under Article 21 of the Constitution of India as recognised in Justice K.S. Puttaswamy v Union of India (2017). Despite the enactment of the Digital Personal Data Protection Act 2023, India has no dedicated deepfake legislation, no algorithmic accountability framework, and a data protection regime that remains unoperationalised. Drawing on the EU General Data Protection Regulation, the EU Artificial Intelligence

Act 2024, and China's Personal Information Protection Law, this paper argues for urgent legislative reform to give constitutional privacy rights genuine and enforceable content in the age of AI companions and generative surveillance.

Keywords: *Article 21, right to privacy, AI companions, AI trend, deepfakes.*

INTRODUCTION

Type "create a boyfriend/girlfriend for me" into ChatGPT. Within seconds, a face appears: dark eyes, a half-smile, a realistic person. The AI gives him/her a personality, a backstory, and preferences. It begins a conversation. For the user, it feels private, intimate, almost confessional. What the interface is carefully designed to prevent her/him from thinking about is what is actually happening on the other side of that screen. Every word she/he types is being stored and processed. There are growing concerns that generative AI systems trained on large-scale internet datasets may reproduce features resembling real individuals without their knowledge or consent. The conversation she/he believes is disappearing into a synthetic companion is, in legal reality, being fed into a data processing pipeline operated by a company incorporated in a foreign country, subject to foreign law, with interests entirely distinct from her/his own.

This is not a hypothetical. In 2023 and 2024, AI companion applications Replika, Chai,[1] and dozens of similar platforms recorded explosive growth in India, particularly among young adults. The trend of asking generative AI tools to create romantic partners, synthetic friends, and personalised emotional companions became a documented social phenomenon, with tens of millions of interactions occurring globally. Simultaneously, tools like ChatGPT,[2] DeepSeek,[3] and Meta AI[4] were being used by Indian users to generate photorealistic human faces, sometimes faces bearing an unmistakable resemblance to real individuals whose photographs had been used without consent to train these models. The Ministry of Electronics and Information

[1] 'Privacy Policy' (*Chai Research*, 19 May 2026) <https://www.chai-ai.com/privacy> accessed 24 May 2026
[2] 'Privacy Policy' (*OpenAI*, 28 April 2026) <https://openai.com/policies/privacy-policy> accessed 24 May 2026
[3] 'DeepSeek Privacy Policy' (*DeepSeek*, 10 February 2026) <https://cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html> accessed 24 May 2026
[4] 'Privacy Policy' (*Facebook*, 16 December 2025) <https://www.facebook.com/privacy/policy/> accessed 24 May 2026

Technology issued an advisory on deepfakes in November 2023, acknowledging the harm but offering no enforceable remedy.[5]

These are not isolated technological curiosities. They are the most visible and emotionally immediate manifestations of a far broader and more systematic crisis: the large-scale surveillance, recording, and behavioural profiling of individuals by AI platforms embedded in daily life. When a user searches for something on YouTube and finds the same theme appearing in their Instagram feed within hours, when a private conversation about a product translates into a targeted advertisement before the day is out, this is not a coincidence. It is architecture. And it is architecture that raises a direct constitutional question under Article 21 of the Constitution of India.[6]

The constitutional foundation is not disputed. The nine-judge bench of the Supreme Court in Justice K.S. Puttaswamy v Union of India[7] unanimously held that privacy is a fundamental right, not a legislative concession, but an attribute of personhood that the Constitution protects. Justice Chandrachud identified informational privacy, decisional autonomy, and the protection of identity as core dimensions of that right.[8][9] Justice Kaul grounded the entire framework in dignity, the foundational constitutional value that demands every individual be treated as a full moral person, not as a data point to be extracted and monetised.[10] The Supreme Court has also affirmed in National Legal Services Authority v Union of India[11] that the right to identity is a component of the right to life and personal liberty under Article 21, a holding with direct application to the AI-generated identity appropriation this paper describes.

The real issue is how the law should respond when AI systems shape identity, behaviour, and choice. The stronger position is that Article 21 requires the State to regulate these practices effectively, while horizontal application may apply in limited cases.

---

[5] 'Union Government issues advisory to social media intermediaries to identify misinformation and deepfakes' (*Press Information Bureau*, 07 November 2026) <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1975445&reg=48&lang=2> accessed 24 May 2026
[6] Constitution of India 1950, art 21
[7] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[8] *Ibid* [168]-[185]
[9] *Ibid*
[10] *Ibid* [638]-[647]
[11] *National Legal Services Authority v Union of India and Ors* (2014) 5 SCC 438

The paper sets out the constitutional architecture of the right to privacy, maps the specific privacy violations of AI companions, generative face tools, and behavioural profiling platforms onto constitutional categories and also analyses India's legislative response through the DPDP Act 2023 and identifies its critical gaps, undertakes comparative analysis drawing on the EU, the United States, and China.

THE CONSTITUTIONAL ARCHITECTURE OF PRIVACY: FROM GOBIND TO PUTTASWAMY

The Doctrinal Journey: Privacy's journey in Indian constitutional law was long and contested. The early Supreme Court decisions in M.P. Sharma v Satish Chandra and Kharak Singh v State of Uttar Pradesh cast doubt on whether privacy could be recognised as a fundamental right, since the framers had deliberately omitted it. Gobind v State of Madhya Pradesh[12] marked the first tentative judicial recognition of a right to privacy, locating it in Article 21 but leaving its doctrinal foundations uncertain. Maneka Gandhi v Union of India[13] transformed the interpretive landscape, establishing that Article 21 protects not merely the fact of personal liberty but demands that any restriction on it satisfy the requirements of fairness, justice, and reasonableness.

The definitive resolution came in August 2017. In Justice K.S. Puttaswamy v Union of India,[14] All nine judges agreed that privacy is a fundamental right guaranteed by the Constitution. The bench identified privacy as multi-dimensional, encompassing not merely the physical space of the home but the psychological space of the individual: her thoughts, her relationships, her data, and her identity. Justice Chandrachud's opinion articulated three dimensions with particular relevance to AI: informational privacy, the right to control data about oneself; decisional autonomy, the right to make choices free from manipulation; and contextual integrity, the norm that personal information shared in one context should not flow to incompatible contexts without consent.[15][16]

[12] *Gobind v State of Madhya Pradesh and Anr* (1975) 2 SCC 148
[13] *Maneka Gandhi v Union of India* (1978) 1 SCC 248
[14] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[15] *Ibid* [168]-[185]
[16] *Ibid*

Two further principles from Puttaswamy anchor this paper's analysis. First, the right to informational self-determination, the individual's ability to control what is known about them and how that knowledge is deployed, is a constitutionally protected component of the right to privacy.[17] Second, any restriction on the right must satisfy the proportionality standard: it must pursue a legitimate aim, be rationally connected to that aim, be the least restrictive means available, and strike a fair balance between the aim pursued and the right restricted.[18] Both principles are directly engaged by the AI practices. The Supreme Court's subsequent recognition in Namit Sharma v Union of India[19] of dignity and identity as components of Article 21 further strengthens the constitutional basis for regulating AI-generated identity appropriation.

The Application of Article 21 to Private AI Companies: A threshold objection must be addressed. Fundamental rights under Part III bind the State as defined in Article 12 of the Constitution.[20] Private technology companies, Meta, OpenAI, Replika, and DeepSeek are not State actors. Does Article 21 have any constitutional bearing on their conduct?

The answer operates through two pathways. The first is the State's positive obligation to legislate. The Supreme Court in Vishaka v State of Rajasthan[21] held that the State's failure to enact legislation protecting women from sexual harassment at the workplace was itself a violation of fundamental rights. The same logic applies to AI surveillance: Parliament's failure to create a comprehensive, enforceable data protection regime that genuinely covers AI companies, including their companion applications, generative tools, and algorithmic profiling systems, is a failure of the State's constitutional obligation under Article 21. The gaps in that regime are constitutional failures, not mere policy shortcomings.

The second pathway operates through the DPDP Act 2023, which imposes statutory obligations on private data fiduciaries, including foreign AI companies that offer services to persons in India.[22] The Act translates the constitutional right into enforceable statutory duties. The problem explored in this paper is that the Act has not yet been fully operationalised, leaving the

[17] *Ibid* [298]
[18] *Ibid* [310]-[316]
[19] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2019) 1 SCC 1
[20] Constitution of India 1950, art 12
[21] *Vishaka and Ors v State of Rajasthan and Ors* (1997) 6 SCC 241
[22] Digital Personal Data Protection Act 2023, s 3

constitutional right without effective enforcement machinery in the precise context where it is most urgently needed.

AI COMPANIONS, SYNTHETIC FACES, AND BEHAVIOURAL SURVEILLANCE: THE ANATOMY OF PRIVACY VIOLATION

The AI Boyfriend/Girlfriend Phenomenon and the Intimacy of Data: The AI companion trend deserves careful legal attention precisely because it has received so little of it in Indian legal scholarship. When a user opens Replika or a similar application and begins sharing her/his innermost thoughts with a synthetic partner, she/he is not merely having a conversation. She/He is feeding an intimate data stream to a commercial operation whose business model depends on the accumulation and exploitation of exactly that intimacy.

Replika's privacy policy discloses that it collects the full content of user conversations, usage data, device information, and, depending on the subscription tier, voice data and images shared by users. This data is used for model training, product development, and, in some versions of the policy, sharing with third-party partners.[23] The user who believes she/he is confiding in a private synthetic companion is, in legal reality, providing detailed psychological data to a commercial entity with interests entirely distinct from her/his own. Privacy scholars have noted that this genre of data, emotional, therapeutic, and relational, is particularly sensitive because of its potential for manipulation and its intimate connection to the individual's inner life.[24]

The constitutional concern is substantial and warrants scrutiny. The user has shared information in the specific context of an intimate, therapeutic, and emotionally private relationship. The norm of contextual integrity recognised in Puttaswamy as a dimension of the right to privacy demands that information shared in one context not be deployed in a fundamentally incompatible one. When that intimate conversation data is extracted, stored on foreign servers, used to train commercial models, and potentially shared with third parties, the contextual norm is violated in the most direct possible way.

There is a further dimension that distinguishes the AI companion violation from ordinary commercial data collection. The AI companion is specifically designed to elicit emotional

[23] *Ibid*
[24] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010) 127-39

disclosure to create the psychological conditions of trust and intimacy that cause individuals to share more deeply than they would in any transactional context. This is not incidental to the business model; it is the mechanism. An AI system engineered to lower the user's informational guard to extract deeper data is not merely collecting personal information; it is manipulating decisional autonomy, which Puttaswamy recognised as a constitutionally protected interest.[25]

Generative AI and the Non-Consensual Creation of Identities: The second privacy violation this paper addresses is the use of generative AI to produce photorealistic human faces, including faces that resemble or are derived from real, identifiable individuals without their knowledge or consent. When ChatGPT or a similar tool generates a realistic human face, it draws on a training dataset typically consisting of millions of photographs scraped from the internet without consent from the individuals depicted.[26] The face produced may not be identical to any single person, but it may be sufficiently similar to an identifiable individual to be recognisable to those who know them.[27]

Used in a romantic or sexual context, as the AI companion trend increasingly involves, this may constitute a form of identity appropriation that is qualitatively distinct from prior forms of privacy violation. The Ministry of Electronics and Information Technology acknowledged the seriousness of this harm in its November 2023 advisory on deepfakes. But an advisory creates no legal right and no enforceable remedy. The existing statutory framework is inadequate: Section 66E of the Information Technology Act 2000 punishes the capture and publication of private visual images without consent, but does not address the generation of synthetic likenesses from biometric training data. The Intermediary Guidelines of 2021 require platforms to remove non-consensual intimate imagery, but provide no remedy for the generation of synthetic content from scraped biometric data in the first place. India has no dedicated deepfake legislation, no personality rights statute, and no civil remedy specifically designed for individuals whose likenesses are appropriated by generative AI.

[25] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [168]-[185]
[26] Kashmir Hill, 'This Tool Could Protect Your Photos From AI Manipulation' *The New York Times* (03 August 2023) <https://www.nytimes.com/2020/08/03/technology/fawkes-tool-protects-photos-from-facial-recognition.html> accessed 24 May 2026
[27] *Ibid*

The constitutional analysis is clear. The Supreme Court in National Legal Services Authority v Union of India[28] held that the right to identity, the right of every individual to have their identity recognised and protected, is a component of the right to life and personal liberty under Article 21. Justice Kaul's opinion in Puttaswamy grounded the right to privacy in dignity, the constitutional value that demands every individual be treated as a full moral agent, not as raw material for another's commercial purposes.[29] The non-consensual use of a person's biometric data to generate their synthetic likeness, particularly in intimate or romantic contexts, is an affront to both identity and dignity in their most direct constitutional sense.[30]

The European Union has recognised this category of harm and responded to it through its classification of biometric data as a special category of personal data attracting heightened protection under Article 9 of the GDPR.[31] The UK Court of Appeal in R (Bridges) v Chief Constable of South Wales Police[32] held that facial recognition technology must comply with data protection law and human rights obligations. India has neither a special category framework for biometric data nor any judicial ruling addressing the specific privacy implications of generative AI and synthetic faces. This is a gap that Indian courts and Parliament must urgently address.

Behavioural Surveillance and Algorithmic Profiling: The AI companion and synthetic face phenomena are the most emotionally immediate forms of AI privacy violation, but the most pervasive is the continuous, cross-platform behavioural surveillance that Meta, YouTube, Instagram, and similar platforms conduct as a matter of routine commercial practice.

Meta's privacy policy discloses that it collects data about content users create, share, and interact with; the networks and relationships they maintain; location data derived from devices; and information about websites and apps that use Meta's technologies, meaning that Meta tracks user behaviour across the internet, not merely on its own platforms. Every search, every pause, every scroll, every reaction is recorded and fed into a profiling system of extraordinary granularity. OpenAI reserves the right to use conversation content for model training unless users opt out through a process most users do not know exists.[33] DeepSeek, whose rapid rise in

[28] *National Legal Services Authority v Union of India and Ors* (2014) 5 SCC 438 [66], [71]
[29] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [638]-[647]
[30] *Ibid*
[31] General Data Protection Regulation 2016, art 9
[32] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058
[33] Privacy Policy (n 2)

India in early 2024 made it one of the most downloaded applications in the country, stores all user data, including the full content of conversations, on servers in the People's Republic of China, subject to Chinese law and potentially accessible to Chinese State agencies.

Shoshana Zuboff's analysis of surveillance capitalism describes this architecture with precision: behavioural data is not a by-product of digital services but their primary commercial product collected and processed to generate predictions about future behaviour that are sold to advertisers, political campaigns, and others seeking to influence human conduct.[34][35] The YouTube and Instagram recommendation algorithms exemplify this dynamic. As users engage, the algorithm learns not merely what they have consumed but what emotional states they are susceptible to, what content produces extended engagement, and what might push them toward further interaction. The feed is not a neutral reflection of the user's interests; it is a carefully engineered environment designed to maximise data extraction.[36][37]

Mapped onto the Puttaswamy framework, the violations are systematic. Informational privacy is violated by collection without meaningful consent. Decisional autonomy is violated when algorithmic systems manipulate the user's information environment to nudge behaviour and beliefs. Dignity is violated when persons are reduced to commercial profiles stripped of agency. And identity privacy is violated when data is used to construct representations of individuals that the individual has never endorsed and cannot contest.[38][39] Indian scholars have noted, with justification, that this form of data extraction operates as a kind of digital colonialism, extracting value from Indian users' behavioural data while providing those users with no legal protection over the extraction.[40]

---

[34] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 8-12
[35] *Ibid* 93-97
[36] *Ibid* 199-204
[37] Guillaume Chaslot, 'How Algorithms Can Learn to Discredit "the Media"' (*Medium*, 02 February 2018) <https://guillaumechaslot.medium.com/how-algorithms-can-learn-to-discredit-the-media-d1360157c4fa> accessed 24 May 2026
[38] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [168]-[185]
[39] *Ibid* [638]-[647]
[40] Anita Gurumurthy and Deepti Bharthur, 'DEMOCRACY AND THE ALGORITHMIC TURN' (2018) 15(27) SUR - International Journal on Human Rights 39, 41-45 <https://sur.conectas.org/wp-content/uploads/2018/07/sur-27-ingles-anita-gurumurthy-deepti-bharthur.pdf> accessed 24 May 2026

INDIA'S LEGISLATIVE RESPONSE: THE DPDP ACT 2023 AND ITS CRITICAL LACUNAE

The Long Road to Legislation: India's journey towards data protection legislation has been characterised by delay that reflects the difficulty of legislating against powerful commercial interests. Following Puttaswamy, the Justice Srikrishna Committee produced a detailed report in 2018 recommending a comprehensive data protection framework.[41] A Personal Data Protection Bill was introduced in Parliament in 2019,[42] referred to a Joint Parliamentary Committee for two years, and then was withdrawn in August 2022 without public explanation. The Digital Personal Data Protection Act 2023 was enacted the following year, but its substantive provisions remain pending commencement through notifications that the Government has not yet issued.[43]

The Act establishes a framework of data fiduciaries and data principals, requiring consent for most data processing,[44] mandating transparency about the purposes of collection,[45] and imposing obligations of accuracy, storage limitation, and security safeguards.[46] The Act also provides data principals with rights of erasure.[47] and grievance redressal.[48] These are foundational obligations. But a statute not in force provides no protection, and every month of delay is a month in which the constitutional violations described in Part III continue without remedy.

The Gap on AI Companions, Synthetic Content, and Biometric Data: The most significant gap in the DPDP Act 2023 in the specific context of this paper is its silence on AI companion applications, generative face tools, and synthetic content derived from biometric data. The Act focuses on the processing of personal data and imposes consent and transparency obligations on data fiduciaries. It says nothing about the AI companion business model, in which intimate conversation data is specifically engineered to be elicited rather than merely

[41] Justice BN Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology 2018)
[42] Personal Data Protection Bill 2019
[43] Digital Personal Data Protection Act 2023, s 1(2)
[44] *Ibid* s 6
[45] *Ibid* s 5
[46] *Ibid* ss 8-9
[47] *Ibid* s 12
[48] *Ibid* s 13

incidentally collected.[49] It says nothing about the generation of synthetic likenesses from training datasets containing personal photographs. And it says nothing about the use of AI-generated content in romantic or sexual contexts involving real people's appearances.

The GDPR's treatment of biometric data as a special category attracting heightened protection under Article 9[50] offers the most instructive contrast. Under the GDPR, the processing of biometric data for uniquely identifying a natural person is prohibited absent explicit consent or other specified grounds. India's DPDP Act contains no equivalent provision. The biometric data that generative AI companies scrape from the internet to train face-generation models, photographs of real people, taken in contexts entirely unrelated to AI training, is processed under Indian law without any heightened protection whatsoever.[51]

The Algorithmic Accountability Void: A second critical gap is the complete absence of any provision for algorithmic accountability. The Act does not require AI companies to disclose the logic of automated decision-making. It creates no right to contest algorithmic decisions. It imposes no obligation to explain why a particular user was profiled in a particular way, denied a particular service, or served a particular category of content.[52]

The EU's Artificial Intelligence Act 2024, the world's first comprehensive AI regulation, directly addresses this gap by classifying certain AI systems as high-risk and requiring transparency, human oversight, and the right to explanation for consequential automated decisions.[53] The Act also explicitly prohibits AI systems that deploy subliminal manipulation techniques to distort behaviour in ways that harm individuals, a provision that would directly regulate the architecture of AI companion applications if it applied in India.[54] No comparable provision exists in Indian law. An Indian user who is denied employment through an AI screening tool, manipulated by an AI companion system, or radicalised by a recommendation algorithm has no statutory right to know why, and no legal mechanism to challenge what has been done with their data.

[49] Digital Personal Data Protection Act 2023, ch II
[50] General Data Protection Regulation 2016, art 9
[51] *Ibid* art 4(14)
[52] Digital Personal Data Protection Act 2023
[53] EU Artificial Intelligence Act 2024, art 6 and annex III
[54] *Ibid* art 5(1)(a)

The State Exemption and the Cross-Border Problem: Section 18(2)(a) of the DPDP Act 2023 exempts government instrumentalities from most of the Act's obligations in the interests of national security, public order, and sovereignty.[55] The breadth of this exemption is constitutionally questionable. Puttaswamy held that restrictions on the right to privacy must satisfy the proportionality standard.[56] A blanket exemption for all government AI processing, including the facial recognition surveillance systems that Indian police forces are deploying at scale, does not satisfy this standard and is constitutionally vulnerable to challenge.

The cross-border problem is equally pressing. The Act permits data transfers to countries notified as providing adequate protection[57], but the notification framework has not been established. Indian users' intimate conversation data from AI companion applications and their biometric data scraped for generative face tools flow to servers in the United States, China, and elsewhere without any assessment of the protection available. The specific case of DeepSeek, which stores Indian users' data on Chinese servers, is subject to Chinese law. represents the most urgent and concrete instance of this constitutional gap. The right to informational self-determination that Puttaswamy recognised[58] is, at the cross-border level, entirely unenforced.

A COMPARATIVE LENS: LESSONS FOR INDIA

The European Union: Rights by Design and the AI Act: The European Union's General Data Protection Regulation, in force since May 2018, provides the most instructive regulatory comparator.[59] Its foundational contribution is to shift the burden of compliance onto data controllers, requiring them to demonstrate a lawful basis for processing, implement data protection by design, and maintain records of processing activities. Its five data protection principles are lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; and storage limitation.[60] correspond precisely to the privacy interests Puttaswamy identified.

[55] Digital Personal Data Protection Act 2023, s 17(2)
[56] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [310]-[316]
[57] Digital Personal Data Protection Act 2023, s 16
[58] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [168]-[185]
[59] General Data Protection Regulation 2016, art 9
[60] *Ibid* art 5(1)

Article 22 of the GDPR gives individuals the right not to be subject to decisions based solely on automated processing that produce significant effects concerning them.[61] The right to erasure under Article 17[62] and the CJEU's ruling in Google Spain[63] give individuals the right to demand deletion of data that is no longer necessary. The Schrems ruling[64] establishes that cross-border data transfers require equivalent protection, directly addressing the DeepSeek-China problem that India currently cannot resolve. The GDPR's special category framework for biometric data[65] gives the highest level of protection to exactly the category of data that generative face tools exploit, protection that is absent in Indian law.

The EU Artificial Intelligence Act 2024 goes further still, classifying AI companion systems and emotion-recognition tools as high-risk AI systems requiring conformity assessment, transparency, and human oversight.[66] Its prohibition on AI systems that use subliminal manipulation techniques[67] directly addresses the architecture of companion applications designed to elicit intimate disclosure. India has no equivalent regulatory framework, and the contrast could not be more significant for the tens of millions of Indian users interacting with these systems daily.

The United States and the Cost of Fragmentation: The United States has no comprehensive federal data protection law. Its sectoral approach creates systematic gaps that AI companies exploit readily. The California Consumer Privacy Act 2018[68] is the most advanced domestic instrument, but its limited enforcement mechanisms and its exclusion of employment data leave significant areas unprotected.

The American experience illustrates the cost of fragmentation in the AI era. When behavioural data flows seamlessly across sectors, health data feeding insurance algorithms, location data feeding credit scoring, and conversation data feeding political targeting, sectoral regulation creates gaps that AI companies traverse without difficulty. India has a constitutional advantage the United States lacks: a judicially recognised fundamental right to privacy, providing a unified

[61] *Ibid* art 22
[62] *Ibid* art 17
[63] *Google Spain SL v Agencia Espanola de Proteccion de Datos* [2014] Case C-131/12 (ECLI:EU:C:2014:317)
[64] *Schrems v Data Protection Commissioner* [2015] Case C-362/14 (ECLI:EU:C:2015:650)
[65] General Data Protection Regulation 2016, art 9
[66] EU Artificial Intelligence Act 2024, annex III
[67] *Ibid* art 5(1)(a)
[68] California Consumer Privacy Act 2018, Cal Civ Code ss 1798.100-1798.199

basis for comprehensive regulation.[69] The failure to leverage that advantage through operationalised legislation is a choice with constitutional consequences.

China's PIPL: A Cautionary Model: China's Personal Information Protection Law 2021 imposes comprehensive consent and purpose-limitation requirements and maintains some of the world's most restrictive cross-border transfer rules.[70] On paper, it is a sophisticated privacy statute. In practice, it is a cautionary tale: its comprehensive State exemptions and subordination of individual rights to State interests demonstrate that privacy legislation can be formally comprehensive while providing citizens no genuine protection against the most significant threat they face, which, in many cases, is the State itself.

The concern that India's DPDP Act 2023 partially replicates this structure with its broad government exemptions, executive-appointed regulatory board, and weak civil society consultation mechanisms has been raised persistently by legal scholars and civil liberties organisations.[71] The comparative lesson is straightforward: genuine privacy protection requires the law to apply with equal force to State and private actors alike, and enforcement to be genuinely independent of political control. Legislation designed primarily to manage private competitors rather than to protect individual rights is not privacy law; it is regulatory capture dressed in constitutional language.

RECOMMENDATIONS AND CONCLUSION

Six concrete reforms are required to bring India's legal framework into constitutional adequacy for the age of AI companions and generative surveillance. First, the DPDP Act 2023 must be operationalised without further delay. Every month of delay is a month in which constitutional violations continue without remedy. The Data Protection Board must be constituted with statutory guarantees of independence, security of tenure, protection from executive dismissal, and a transparent merit-based appointment process to ensure it can adjudicate robustly against both private companies and government agencies.

[69] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[70] Personal Information Protection Law of the People's Republic of China 2021
[71] Anushka Jain and Prateek Waghre, 'Comments on the Digital Personal Data Protection Bill 2023' (*Internet Freedom Foundation*, 03 August 2023) <https://internetfreedom.in/statement-dpdpb-2023/> accessed 24 May 2026

Second, Parliament must enact dedicated legislation on AI-generated synthetic content and deepfakes. This legislation should create civil and criminal liability for the non-consensual creation and distribution of synthetic likenesses of identifiable individuals; establish a personality rights framework giving individuals legal control over the use of their faces, voices, and biometric identifiers in AI training datasets; and provide a specific civil remedy for individuals whose likenesses are used in AI companion or generative face applications without consent.

Third, algorithmic accountability provisions must be introduced either through amendment of the DPDP Act or through a standalone AI regulation modelled on the EU AI Act, requiring companies to disclose the logic of automated decisions that significantly affect individuals and giving those individuals a meaningful right of contest. This directly addresses the recommendation algorithm and behavioural profiling practices that raise concerns regarding one of the most pervasive forms of AI surveillance affecting Indian users.

Fourth, AI companion applications must be specifically regulated. Their business model engineering intimacy to extract data constitutes a form of manipulative data processing that goes beyond what a consent-based framework can adequately address. Specific obligations should include a prohibition on the use of intimate conversation data for any purpose other than service delivery; mandatory disclosure that the companion is an AI system; a prohibition on design features specifically intended to elicit emotional dependency; and data localisation requirements for the most sensitive categories of conversation data.

Fifth, the cross-border data transfer framework must be urgently operationalised. An adequacy assessment mechanism must be established, and interim restrictions imposed on transfers to jurisdictions, particularly China, that do not provide equivalent protection. The situation of DeepSeek users who shared intimate personal data with a system storing it on Chinese servers under Chinese law is a specific, immediate, and currently unaddressed constitutional harm.

Sixth, the State exemption in Section 18(2)(a) of the DPDP Act must be narrowed to satisfy the proportionality standard that Puttaswamy requires.[72] Facial recognition systems deployed by

[72] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [310]-[316]

government agencies,[73] AI tools used in welfare determination, and behavioural surveillance systems operated by law enforcement must all be subject to the same consent, purpose-limitation, and proportionality requirements that bind private companies.

CONCLUSION

The person who typed "create a boyfriend/girlfriend for me" into an AI application did not think she/he was making a legal decision. She/He was not thinking about Article 21 or Puttaswamy or the Digital Personal Data Protection Act. She/He was thinking about happiness or just a playful act. And in that ordinary human moment, reaching for connection in a world that increasingly mediates intimacy through screens, she/he was subjected to a set of data extraction, identity manipulation, and surveillance practices that raise serious concerns regarding her/his fundamental rights under Article 21.

The Supreme Court in Puttaswamy held that privacy is not a gift of the State. It is a right that inheres in every person by virtue of their humanity, the right to control what is known about them, to make choices free from manipulation, and to have their identity treated as their own.[74][75] The Supreme Court later confirmed in National Legal Services Authority[76] and the right to be forgotten litigation that Article 21 extends to the protection of identity and informational control in new and evolving contexts. These principles are capacious enough to govern AI companions and synthetic face generation, and the obligation to apply them falls on Parliament, the executive, and ultimately the courts.

India stands at a moment of genuine constitutional consequence. The question is not whether the right to privacy extends to AI surveillance, synthetic identity generation, and companion application data exploitation. Puttaswamy makes clear that it does. The question is whether the institutions of the State will honour that constitutional commitment with the legislative, regulatory, and judicial action it demands. The DPDP Act 2023 is a beginning, imperfect, incomplete, and as yet inoperative. What remains is the harder work: filling the legislative gaps,

[73] Anushka Jain, 'The Increasing Use of Facial Recognition Technology in India' (*Internet Freedom Foundation*, 09 February 2021) <https://internetfreedom.in/the-increasing-use-of-facial-recognition-technology-in-india/> accessed 24 May 2026
[74] *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1 [168]-[185]
[75] *Ibid* [638]-[647]
[76] *National Legal Services Authority v Union of India and Ors* (2014) 5 SCC 438

building independent enforcement institutions, regulating the AI companion trend that millions of Indian users are navigating without legal protection, and recognising that the non-consensual generation of synthetic likenesses raises serious constitutional concerns requiring legislative and judicial attention.

Dr B.R. Ambedkar reminded the Constituent Assembly that constitutional morality is not a natural sentiment; it must be cultivated through deliberate institutional effort.[77] In the age of AI companions, scraped faces, and cross-platform surveillance, cultivating constitutional morality means refusing to accept that the price of digital connection is the surrender of privacy and insisting, as the Constitution requires, that every person retains the right to be known only as they choose to be known.

Watching without warrant, generating without consent, profiling without accountability- these are not the edge cases of constitutional law in the age of artificial intelligence. They are its daily reality. And the law must finally be made to say so.

[77] 'CONSTITUENT ASSEMBLY DEBATES VOLUME 7: 04 NOV 1948' (*Constitution of India*) <https://www.constitutionofindia.net/debates/04-nov-1948/> accessed 24 May 2026