THE DIGITAL DOUBLE: ADDRESSING THE LEGAL LACUNA IN INDIA'S LIKENESS PROTECTION FRAMEWORK

Deepthi Juliana Hariharan*

ABSTRACT

This paper explores a growing legal "black hole" in India: the moment a stranger's face in a public street becomes raw material for AI-driven abuse. While snapping photos in public has long been a legal free-for-all, the rise of generative AI ranging from Grok to predatory "undressing" bots has fundamentally changed the stakes. What used to be an innocent, incidental capture can now be weaponised into sexualized or defamatory content with a few clicks. My research critiques the Digital Personal Data Protection (DPDP) Act, specifically arguing that its exemption for "publicly available data" is a dangerous oversight in the age of deepfakes. By leaving public likenesses unprotected, the law inadvertently gives a green light to digital harassment. To fix this, I propose a new "Right to Likeness Control." Drawing inspiration from more robust legal frameworks in Europe and the UAE, this paper outlines how India can protect its citizens' digital identities without stifling the freedom of public spaces.

Keywords: Digital Personal Data Protection (DPDP) Act, Generative AI, Right to Likeness, Non-Consensual Synthetic Media (NCSM), Publicly Available Data Exemption.

INTRODUCTION

For decades, walking through a crowded Indian bazaar or a public park came with a silent social contract: "Public Anonymity." You might be seen by hundreds of people, but you weren't truly known. If a photographer captured you in the background of a shot, you were merely a "face in the crowd"—an incidental, fleeting moment of light and shadow that would eventually fade into obscurity.

*BBA LLB, FOURTH YEAR, KRISTU JAYANTI COLLEGE OF LAW.

However, in 2026, the nature of light has changed. With the rollout of multi-modal AI models and "democratised" generative tools like Grok and specialised deepfake bots, a single "innocent" photograph is no longer a static memory. It has become a digital seed.

Today, a stranger can capture your likeness in a public space, upload it to a server, and within seconds manipulate your face into pornographic content, defamatory "evidence," or a fraudulent digital avatar. The transition from a "bystander" to a "data point" has happened faster than our laws can keep up.

The primary friction point lies in our current legislation. The Digital Personal Data Protection (DPDP) Act (2023/2025) was a landmark step for India, but it carries a dangerous legacy of the "pre-AI" era: the exemption for publicly available data. Under Section 3, if you are "visible" in public, the law suggests your data might be fair game for processing.[1] This creates a terrifying loophole where the very act of existing in a public space is treated as "implied consent" for digital weaponisation.

THE END OF "PUBLIC ANONYMITY"

The traditional concept of a "public space" as a zone of fleeting interactions is dead. We used to rely on what Professor Helen Nissenbaum calls Contextual Integrity—the idea that privacy isn't just about secrets, but about the appropriate flow of information.[2] When I walk down the street, I expect to be seen by passersby, but I do not expect to be "datafied" and uploaded to a permanent server for AI training. My research finds that the shift from "photography as art" to "photography as data collection" has destroyed the "implied consent" we once granted to street photographers.

THE TECHNOLOGICAL WEAPONISATION OF THE BYSTANDER

The 2025/2026 rollout of multi-modal generative models (like Grok-3 or advanced variants of Stable Diffusion) has turned the human face into a "digital seed." A single high-definition capture of a bystander can now be processed by predatory "nudification" bots or "deep-voice" synthesisers. My findings show a disproportionate impact on women and children in the Indian context, where digital "shaming" has severe socio-cultural consequences. Unlike traditional

[1] Digital Personal Data Protection Act 2023, s 3(c)(ii)
[2] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press 2010) 127

defamation, which is static, AI-driven abuse is **iterative**; it can be recreated and evolved by anyone with a basic API.

CURRENT LEGAL LANDSCAPE IN INDIA (2025-2026)

The DPDP Act 2023 is a double-edged sword. While it creates the "Data Fiduciary" framework, Section 3(c)(ii) creates a massive "Legal Lacuna" by exempting personal data that is made "publicly available."[3] Legal scholars have noted that this allows AI companies to scrape faces from public photos without being technically in breach of the Act. Furthermore, while the MeitY Oct 2025 Amendment to the IT Rules mandates 10% watermarking on AI content, it fails to address the source of the data. My analysis of the Bharatiya Nyaya Sanhita (BNS) 2023 shows that voyeurism laws (Section 77) still require a "private act," ignoring the fact that AI can turn a public act into a private violation.[4]

COMPARATIVE JURISPRUDENCE (GLOBAL MODELS)

To address the "Legal Lacuna" in India, we must look at how global legal systems are grappling with the same AI pivot. I analysed three distinct models that offer a blueprint for protecting bystanders.

The Personality Rights Model: Germany's "Recht am eigenen Bild": Germany provides arguably the most robust protection for the individual likeness through the concept of Recht am eigenen Bild (the right to one's own image), codified in Sections 22 and 23 of the Kunsturhebergesetz (KUG).[5] Unlike the Indian DPDP Act, which focuses on the "processing" of data, German law focuses on the dignity of the image. Section 22 establishes a "consent-first" rule: images may only be distributed or displayed with the express permission of the subject.

While Section 23 offers exceptions for "contemporary historical events" or individuals who are "mere accessories" to a landscape, the German courts have been increasingly protective in the AI era. In the landmark Olaf Scholz Deepfake Case (2024), the Berlin District Court II granted an injunction against an AI-generated video of the Chancellor, emphasising that even "satire" must be recognisable and cannot infringe on naming and personality rights under Article 12 of

[3] Digital Personal Data Protection Act 2023, s 3
[4] Bharatiya Nyaya Sanhita 2023, s 77
[5] Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KunstUrhG), 22, 23

the German Civil Code (BGB).[6] For the bystander, this means that even if a photo is taken in a "public" sphere, the moment it is moved into a "social" or "private" sphere via AI manipulation, it constitutes a severe violation of personal rights, often triggering claims for damages and immediate injunctive relief.

The Zero-Tolerance Model: UAE's Federal Decree-Law No. 34: The United Arab Emirates offers a stark contrast to the unregulated "street photography" culture of the West and India. Article 44 of Federal Decree-Law No. 34 of 2021 (the Cybercrimes Law) represents a "Zero-Tolerance" approach to public photography.[7] The law criminalises the act of taking, copying, or keeping electronic photos of third parties in any public or private place without consent.

This is particularly relevant for the AI-weaponisation argument because it stops the "Digital Seed" at the point of capture. If the initial snap is illegal, the subsequent "undressing" or "morphing" becomes an aggravated offence. Under this framework, violators face a minimum of six months 'imprisonment and fines ranging from AED 150,000 to AED 500,000 (approx. ₹34 Lakhs to ₹1.1 Crore). For deepfakes specifically, the UAE has integrated these privacy protections with Article 40 (Cyber Fraud) and defamation statutes, ensuring that any AI-generated content intended to harm a reputation carries even steeper penalties—up to one year in prison and fines reaching AED 1 Million. This model prioritises the "security of the person" over the "freedom of the lens."

The Targeted AI Model: USA's DEFIANCE Act of 2024: While the US has traditionally favoured the First Amendment and "public space" photography, the surge in non-consensual AI pornography led to the unanimous Senate passage of the DEFIANCE Act (Disrupt Explicit Forged Images and Non-Consensual Edits) in July 2024.[8] This Act is revolutionary because it creates a federal civil cause of action specifically for "digital forgeries."

The DEFIANCE Act allows victims to sue anyone who knowingly creates, distributes, or even "receives" a sexually explicit deepfake without the subject's consent. Crucially, the Act defines a "digital forgery" as any visual depiction created via software or AI that "falsely appears to be authentic." Unlike Indian law, which struggles to categorise AI harm as "voyeurism" (which usually requires a private act), the US model focuses on the lack of consent to the depiction

[6] Bürgerliches Gesetzbuch (BGB), 12
[7] UAE Federal Decree-Law No 34 of 2021 on Combatting Rumours and Cybercrimes, art 44
[8] Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act of 2024, S 3696, 118th Cong (2024)

itself. It empowers victims to seek statutory damages and the removal of content, regardless of whether the original "seed" photo was taken in a public square or a private bedroom. This targeted approach fills the specific gap where AI turns "innocent" capture into "predatory" output.

IDENTIFYING THE "LEGAL LACUNA"

The "Public Space Fallacy" is the core of the problem. Indian courts, following K.S. Puttaswamy (2017), recognised privacy as a fundamental right, yet the DPDP Act treats public visibility as a waiver of that right.[9] The "Consent Paradox" is that while you cannot "consent" to every stranger's camera, that lack of consent is currently being interpreted by the law as a "voluntary disclosure." This is a fundamental misinterpretation of how AI changes the "harm scale" of a photo.

THE PROPOSED "LIKENESS PROTECTION FRAMEWORK"

To address the identified legal "black hole," this paper proposes a tripartite legislative framework aimed at transitioning India from a passive data regime to an active "Likeness Control" model.

Proposal 1: Statutory Right to Withdrawal: I propose a legal provision allowing individuals to demand the removal of their identifiable likeness from any digital platform, regardless of whether the original capture was "illicit" or taken in a public space. This Right to Withdrawal is distinct from the "Right to be Forgotten" as it focuses on the continued use of one's physical identity rather than just past information.

Legal Basis: This draws from the principle of "Inviolate Personality" originally articulated by Warren and Brandeis as the foundation of privacy rights.[10] It reinforces the "Right to be Let Alone" upheld in Justice KS Puttaswamy v Union of India.[11]

Proposal 2: AI Input Liability: The burden of deepfake prevention must shift from the victim to the platform. We must legislate AI Input Liability, requiring Data Fiduciaries (such as X/Grok or Meta) to implement "Consent Verification" filters. AI tools should be prohibited

[9] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1
[10] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4(5) Harv L Rev 193
[11] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1

from executing "edit," "morph," or "undress" commands on identifiable human faces unless the system verifies the subject's authorisation.

Legal Basis: This aligns with the "Privacy by Design" foundational principles,[12] and mirrors the MeitY 2024 Advisory, which requires intermediaries to ensure AI models do not permit unlawful content.[13] It also adopts the "Safety by Design" principles promoted by global regulators like the Australian eSafety Commissioner.[14]

Proposal 3: Criminalising the "AI Request" (Anticipatory Offence): Current Indian law, such as Section 77 of the Bharatiya Nyaya Sanhita (BNS), focuses on the publication of voyeuristic content. However, the harm often begins at the point of intent. I propose criminalising the "Request for Manipulation"—the act of uploading a stranger's photo with the instruction to generate non-consensual synthetic media—as a standalone offence, regardless of whether the output is shared.

Legal Basis: This reflects the "Inchoate Crime" doctrine, where the law punishes steps taken toward a crime. It builds upon the Information Technology (Intermediary Guidelines) Rules 2021 and is inspired by the targeted civil remedies in the US DEFIANCE Act 2024,[15] adapting them into a criminal deterrent.

CONCLUSION

The findings of this research suggest that we are at a critical crossroads in Indian digital jurisprudence. For too long, the law has relied on a binary "Public vs. Private" distinction that is no longer fit for purpose. As this paper has demonstrated, the transition from a physical bystander to a "digital seed" happens in an instant, but the resulting harm fueled by generative AI can last a lifetime.

My analysis of the DPDP Act (2023/2025) reveals a dangerous "legal vacuum." By exempting publicly available data, we have inadvertently created a loophole that protects the scraper and the manipulator rather than the citizen. While the IT Rules (2025) and watermarking mandates are steps in the right direction, they are merely band-aiding on a deeper wound. They treat the

[12] Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (Information and Privacy Commissioner of Ontario 2009)
[13] Ministry of Electronics and Information Technology (MeitY), 'Advisory to Intermediaries on AI Models' (1 March 2024, revised 15 March 2024)
[14] eSafety Commissioner (Australia), 'Safety by Design Principles' (2024)
[15] Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act of 2024 (USA) S 3696

symptoms of AI abuse rather than the source: the non-consensual capture and data-fication of our physical selves.

By looking at the "Right to one's own image" in Germany, the zero-tolerance privacy laws of the UAE, and the targeted civil remedies of the US DEFIANCE Act, it becomes clear that India's path forward must involve a fundamental shift. We must move toward a "Right to Likeness Control." This isn't about banning photography or stifling innovation; it's about acknowledging that in 2026, our faces are our most sensitive data points.

As a student of law observing this rapid technological shift, I believe the "Consent Paradox" must be resolved. We cannot continue to treat public visibility as a waiver of bodily autonomy. If the law fails to evolve, we risk a future where the simple act of walking down a street makes us "fair game" for digital assault. It is time for the Indian legislature to close the 3(c)(ii) loophole and ensure that while we may be seen in public, our digital identities remain unapologetically our own.