



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

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.

REGULATING VIRTUAL INFLUENCERS IN INDIA: A LEGAL ANALYSIS OF AI-GENERATED PERSONALITIES UNDER CONSUMER AND MEDIA LAWS

Shaurya Shandilya

ABSTRACT

The rapid evolution of digital marketing has driven the rise of virtual influencers AI-generated, computer-generated imagery (CGI) personalities that simulate human behaviours, styles, and interactions. In India, brands increasingly leverage these synthetic personas to engage consumers, presenting unique advantages in cost-efficiency and creative control. However, this shift complicates the regulatory landscape, as AI-generated personalities challenge traditional legal frameworks fundamentally built around human actors.¹

This research paper addresses the core problem of legal accountability and consumer deception, investigating how virtual influencers frequently blur the line between authentic human endorsement and automated marketing. Employing a qualitative and doctrinal methodology, this study analyzes existing legal mechanisms, specifically focusing on the Consumer Protection Act (2019), the Central Consumer Protection Authority (CCPA) Guidelines for Prevention of Misleading Advertisements and Endorsements (2022), and the Advertising Standards Council of India (ASCI) code.²

The main findings indicate a critical enforcement gap: current laws mandate disclosure of commercial relationships but fail to adequately address the inherent synthetic nature of the endorser. This lack of explicit statutory categorization leaves consumers vulnerable to

¹ Chloe S. Agas, Note, *The Real Liability of Virtual Influencers*, 13 J. Bus. Entrepreneurship & L. 121, 121–23 (2020).

² Consumer Protection Act, No. 35 of 2019, India Code; Cent. Consumer Prot. Auth., *Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements* (2022).

deceptive practices, particularly regarding "personal experience" claims for physical products by entities incapable of consuming them. Furthermore, ambiguity persists regarding liability allocation among the AI creators, marketing agencies, and platforms.

To bridge these regulatory fissures, this paper suggests comprehensive legal reforms. It proposes rendering mandatory "AI-generated" watermarks and explicit disclosures on all promotional content, amending consumer laws to establish strict vicarious liability for creators, and creating specialized ASCI frameworks tailored to synthetic media. Ultimately, the study advocates for a balanced regulatory approach that safeguards consumer trust without stifling technological innovation in India's expanding digital economy.

INTRODUCTION

The landscape of digital marketing has undergone a radical transformation. Influencer marketing evolved from early blog endorsements into a multi-billion-dollar global industry built on the currency of human authenticity, relatability, and trust. However, the creator economy is experiencing its most disruptive shift yet: the entry of Artificial Intelligence. No longer confined to backend algorithms, AI has stepped into the spotlight, transforming from a tool used by human creators into the creator itself.

This technological leap has catalyzed the global rise of virtual influencers—computer-generated, AI-driven personas that look, speak, and interact like real people. Globally, pioneer personas like Lil Miquela and Shudu have amassed millions of followers, proving that digital audiences can form deep parasocial relationships with pixels. Recognizing this engagement, brands are rapidly adopting synthetic personalities.³ Virtual influencers offer unprecedented creative control, are entirely immune to real-world scandals, and can operate across multiple digital spaces simultaneously, making them highly lucrative marketing assets.

RESEARCH FRAMEWORK

As these non-human entities become mainstream in India's digital ecosystem, they challenge the foundational assumptions of media and commercial law. This study investigates the friction between synthetic marketing and consumer rights through the following framework:

- **RESEARCH QUESTIONS:**

³ See generally David C. Giles, *Parasocial Interaction: A Review of the Literature and a Model for Future Research*, 4 Media Psychol. 279 (2002).

1. How do existing Indian consumer protection and media laws apply to commercial endorsements made by non-human entities?
 2. Where do the legal liabilities rest when a virtual influencer disseminates misleading or deceptive advertisements?
- **OBJECTIVES OF THE STUDY:** To analyze the current regulatory gaps regarding AI-generated personalities under Indian law, evaluate the adequacy of disclosure norms, and propose a robust legal framework that balances technological innovation with consumer protection.
 - **SCOPE AND LIMITATIONS:** This legal analysis focuses primarily on Indian consumer law (Consumer Protection Act 2019, CCPA Guidelines) and advertising codes (ASCI). It strictly examines virtual influencers used for commercial endorsements, excluding broader AI deepfakes used in political disinformation or non-commercial art. The study is limited by the fast-evolving nature of AI technology and the current lack of specific judicial precedents in India regarding synthetic endorsers.

THE CENTRAL LEGAL PARADOX: Traditional consumer and media laws are inherently anthropocentric; they regulate the conduct, intent, and honesty of *human* influencers. By decoupling the act of endorsement from a living human being, virtual influencers create an unprecedented legal vacuum where accountability becomes fluid and difficult to enforce.

When a human influencer endorses a skincare product, the law assumes a baseline of personal experience and physical liability. A virtual influencer, possessing no physical body, cannot experience a product, yet its creators can code it to simulate a heartfelt recommendation. This separation of the persona from the legal person behind it tests the limits of India's current legal architecture.

UNDERSTANDING VIRTUAL INFLUENCERS AND AI-GENERATED PERSONALITIES

2.1 MEANING AND CONCEPT

A virtual influencer is a computer-generated, fictional digital persona designed to simulate human behaviors, physical aesthetics, and social interactions across digital platforms for commercial, promotional, or entertainment purposes. While traditional social media

influencers rely on lived physical experiences,⁴ virtual influencers are entirely synthetic creations.

The legal distinction between AI influencers and standard Computer-Generated Imagery (CGI) characters rests on autonomous operational capacity. Standard CGI characters (such as cinematic or video game protagonists) are structurally static assets requiring manual frame-by-frame rendering and human scripting for every visual or text output. Conversely, AI influencers integrate algorithmic automation, processing real-time consumer data, generating dynamic content variations, and deploying Natural Language Processing (NLP) to converse directly with followers under variable autonomous conditions.

2.2 TECHNOLOGY BEHIND VIRTUAL INFLUENCERS

The synthesis of virtual influencers relies on an interlocking stack of advanced computational fields:

- Computer-Generated Imagery (CGI): The foundational layer utilizing 3D modeling, spatial wireframing, and photorealistic skin shading to render the character's physical likeness.
- Artificial Intelligence (AI) and Machine Learning (ML): The algorithmic engine enabling the persona to identify, analyze, and assimilate digital cultural trends and consumer preference metrics to optimize audience engagement.
- Generative AI: Specialized algorithmic frameworks, including Generative Adversarial Networks (GANs) and Diffusion models, capable of synthesizing novel, ultra-realistic image sets, motion videos, and contextual scripts without requiring physical photoshoots.
- Deep Learning: Neural network architectures trained on multi-modal datasets that power realistic facial mapping, dynamic voice synthesis, and real-time motion capture translations.⁵

2.3 TYPES OF VIRTUAL INFLUENCERS

Virtual influencers broadly manifest across four conceptual frameworks:

⁴ Agas, *supra* note 1, at 122.

⁵ See Byron Reeves & Clifford Nass, *The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places* (1996).

- Fully AI-Generated: Entities completely driven by automated pipelines, where automated loops formulate visual assets, captions, and localized dialogue updates.
- Human-Controlled Digital Avatars: Digital skins superimposed over physical human actors, utilizing spatial motion capture and voice acting to maintain human agency behind a synthetic facade.
- Brand-Owned Virtual Influencers: Proprietary intellectual property created directly by corporate marketing departments to serve as permanent, controversy-immune brand ambassadors.
- Metaverse Influencers: Spatial personas engineered natively for three-dimensional Web3 environments, augmented reality integrations, and interactive virtual reality platforms.

2.4 FAMOUS EXAMPLES

GLOBAL PERSONALITIES

- Lil Miquela: Created by Brud in 2016, she stands as a milestone 19-year-old Brazilian-American model boasting millions of followers, major fashion sponsorships, and serialized pop music releases.
- Shudu Gram: Engineered by visual artist Cameron-James Wilson as the world's first virtual supermodel, showcasing hyper-realistic, high-fashion aesthetic standards.
- Imma: A high-fidelity Japanese virtual girl with a distinctive pink bob, deeply embedded in Tokyo's street culture and luxury lifestyle sectors.⁶

INDIAN MARKET EXAMPLES

- Kyra: Launched in January 2022 by FUTR Studios, Kyra is recognized as India's pioneer virtual influencer, producing lifestyle and fitness content while executing campaigns for major national brands.
- Naina Avtr: Created by Avtr Meta Labs, she is portrayed as a 20-year-old from Jhansi pursuing Bollywood aspirations, successfully conducting celebrity interview segments and commercial product cross-promotions.

⁶ See *Virtual Influencer*, Wikipedia, https://en.wikipedia.org/wiki/Virtual_influencer (last visited May 31, 2026).

The Hyper-Reality Paradox: Virtual influencers fundamentally blur the distinction between reality and simulation. By interspersing hyper-realistic human imperfections into fully coded digital environments, these entities construct a simulated authenticity that challenges the cognitive boundaries of consumer perception.

THE RISE OF SYNTHETIC AUTHENTICITY: HOW VIRTUAL INFLUENCERS GAIN CONSUMER TRUST

3.1 PSYCHOLOGY OF CONSUMER TRUST AND PARASOCIAL RELATIONSHIPS

The mechanism by which human consumers extend trust to non-human entities is rooted in the cognitive framework of **parasocial interaction**—a psychological phenomenon where an audience member develops a unilateral, perceived intimate relationship with a media persona.⁷ In the digital ecosystem, these parasocial bonds are amplified. While historical media figures maintained structural distance via television or cinematic screens, virtual influencers occupy the exact social feeds as consumers' real-world peers.

This architectural proximity tricks the human brain's evolutionary social triggers. Because human cognition is structurally unequipped to seamlessly differentiate between mediated human contact and high-fidelity algorithmic simulation, consumers experience real affective responses. The persona's perceived availability, curated responsiveness, and manufactured vulnerability evoke feelings of intimacy and consistency, establishing a psychological baseline of commercial trust that equals—and occasionally exceeds—human influencers.⁸

3.2 AI-DRIVEN ENGAGEMENT AND ALGORITHMIC PERSONALITIES

Unlike human creators, whose digital interactions are constrained by physical exhaustion and cognitive bandwidth, virtual influencers utilize an **algorithmic personality** model. Powered by Machine Learning pipelines, these entities execute high-frequency, dynamic data analyses of audience engagement metrics. Generative AI models parse comment sections, track shifting regional slang, and gauge user sentiment in real time, enabling the persona to adapt its tone, values, and visual presentations dynamically.

By removing the friction of human fatigue, an AI-driven personality maintains a state of hyper-personalized, persistent interaction. It optimizes every caption, aesthetic choice, and message

⁷ David C. Giles, *Parasocial Interaction: A Review of the Literature and a Model for Future Research*, 4 Media Psychol. 279, 280–82 (2002).

⁸ Byron Reeves & Clifford Nass, *The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places* (1996).

reply to trigger maximum psychological alignment with targeted demographics, executing a systematically optimized simulation of empathy.

3.3 THE CONCEPT OF SYNTHETIC AUTHENTICITY

This paper introduces the concept of "**Synthetic Authenticity**" to define the artificially engineered trust, vulnerability, and relatability systematically generated through algorithmic feedback loops and scripted digital storytelling. Traditional commercial frameworks treat authenticity as an organic, immutable property tied directly to human lived experiences and moral agency. Conversely, *Synthetic Authenticity* is a manufactured, optimized commodity.

DEFINING SYNTHETIC AUTHENTICITY: The strategic deployment of computational algorithms, data analytics, and fictional narratives to construct a photorealistic persona that simulates human vulnerability, fallibility, and social values, thereby evoking genuine consumer empathy and commercial trust without an organic substrate.

This operationalized authenticity relies on intentional imperfections—such as a virtual model posting a simulated "bad hair day" image, discussing artificial emotional anxieties, or taking stances on socio-political issues. These narrative arc points are calculated inputs designed to mirror human life cycles. By substituting real lived experiences with highly precise digital narratives, synthetic authenticity decouples the commercial value of trustworthiness from the necessity of human existence.

VIRTUAL INFLUENCERS AND THE TRANSFORMATION OF DIGITAL ADVERTISING

4.1 SHIFT FROM CELEBRITY ENDORSEMENTS AND ECONOMIC ADVANTAGES

The commercial architecture of digital advertising has fundamentally shifted from a reliance on human celebrity endorsements to the integration of synthetic personas. Historically, corporate entities accepted significant financial and structural liabilities when contracting with human celebrities or traditional influencers. These risks include physical behavioral scandals, unpredictable public statements, scheduling conflicts, aging, and high contract premiums. Virtual influencers eliminate these human friction points entirely.⁹

⁹ Chloe S. Agas, Note, *The Real Liability of Virtual Influencers*, 13 J. Bus. Entrepreneurship & L. 121, 126 (2020).

From an economic perspective, synthetic personalities operate as highly cost-efficient assets with immense creative control. A brand-owned virtual influencer requires an initial design capital outlay but carries near-zero marginal cost for subsequent international campaigns, eliminating the ongoing expenses of travel, physical photography studios, and recurring talent residuals. Furthermore, because these entities are entirely corporate-controlled intellectual properties, their messaging is mathematically precise. Every gesture, verbal cadence, and background element can be modified in post-production to match exact corporate branding guidelines, removing the risk of unpredictable human behavior.

4.2 DATA-DRIVEN TARGETING AND PERSONALIZED ADVERTISING

Beyond simple visual modeling, virtual influencers represent a fundamental shift toward hyper-targeted, algorithmic marketing. Traditional human influencers push uniform commercial broadcasts out to a broad audience. In contrast, virtual influencers can be dynamically integrated directly into predictive data analytics pipelines. By continuously parsing demographic profiles, consumer metadata, search histories, and digital interaction loops, the synthetic persona can alter its visual aesthetics, wardrobe, spoken languages, and cultural idioms in real-time to match specific target subcultures.

This flexibility enables highly personalized advertising. A singular virtual entity can be rendered simultaneously across multiple geographies, endorsing local products with localized accents and contextually custom backgrounds to disparate micro-segments of consumers.¹⁰

4.3 THE FUTURE OF AI MARKETING: PROGRAMMABLE ADVERTISING SYSTEMS

The Structural Shift: Virtual influencers are not merely digital endorsers; they are fully programmable, self-optimizing advertising systems. They unify content creation, target consumer profiling, and data deployment within a single, continuous computational architecture.

As generative AI and spatial Web3 environments mature, the future of marketing points toward hyper-autonomous, real-time consumer engagement. Future iterations of synthetic influencers will not be restricted to pre-rendered image uploads or static video feeds. Instead, they will act as responsive, conversational agents. They can hold millions of simultaneous,

¹⁰ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

highly personalized interactive streams with individual consumers inside immersive, digital spaces, dynamically modifying their persuasive narratives based on the real-time biometric and sentimental feedback of each viewer.

CONSUMER PROTECTION CHALLENGES UNDER INDIAN LAW

5.1 LEGISLATIVE FRAMEWORK AND REGULATORY FRICTION

The primary legislative mechanism safeguarding consumer interests in India's digital economy is the **Consumer Protection Act, 2019 (CPA)**, supplemented by the **Central Consumer Protection Authority (CCPA) Guidelines for Prevention of Misleading Advertisements and Endorsements, 2022**. The CPA fundamentally modernized Indian consumer law by codifying provisions against "misleading advertisements" and "unfair trade practices" within digital marketplaces.¹¹

Under Section 2(28) of the CPA, an advertisement is misleading if it falsely describes a product, guarantees performance without scientific validation, or deliberately conceals material information. To enforce accountability, the CCPA Guidelines impose strict **endorser liability**, requiring individuals featured in advertisements to conduct due diligence to verify claims before public broadcast.

5.2 THE ANTHROPOCENTRIC LEGAL VACUUM

The integration of virtual influencers creates critical friction within this statutory architecture. Because existing provisions assume a human actor possessing moral agency, legal personhood, and physical sensory capacities, they fail to adequately address AI-generated personalities. This mismatch manifests across three core legal questions:¹²

1. CAN AN AI PERSONALITY BE CONSIDERED AN "ENDORSER"?

Under current statutory definitions, an endorser is envisioned as a legal person—either an individual human or a corporate entity. The CCPA Guidelines define an endorser as an individual or group whose opinions or beliefs reflect the commercial message. Because a virtual influencer is merely an lines of code or a CGI asset, it lacks **juristic personality** (the legal status of having rights and duties). Consequently, the synthetic persona itself cannot

¹¹ Consumer Protection Act, No. 35 of 2019, §§ 2(28), 21, India Code.

¹² Cent. Consumer Prot. Auth., *Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements* (2022).

technically execute due diligence or form a legally cognizable "opinion," placing it outside the literal definition of an endorser.

2. CAN CONSUMERS SUE A VIRTUAL INFLUENCER?

No. Because a virtual entity lacks legal personhood, it cannot sue or be sued in a court of law. A consumer harmed by a misleading product recommendation cannot name a digital persona as a counter-party in a Consumer Disputes Redressal Commission.

3. WHO BEARS LIABILITY?

Since the virtual influencer cannot bear liability, accountability must be legally imputed to the actors behind the simulation. This creates a highly complex, fragmented liability chain under the law:

- **The AI Creators/Developers:** The software engineers or digital artists who code and render the persona.
- **The Marketing Agencies:** The intermediaries managing the persona's commercial contracts and scripting its brand campaigns.
- **The Deploying Brands:** The corporate entities financing the synthetic advertisement.

5.3 UNFAIR TRADE PRACTICES AND DIGITAL RIGHTS

This legal vacuum directly facilitates **unfair trade practices** in the digital marketplace. When a virtual influencer asserts that a specific cosmetic cream "cleared its skin" or a fitness supplement "increased its stamina," the advertisement engages in structural deception. A synthetic entity possesses no physical skin or biology; it is incapable of product consumption or sensory evaluation.

By simulating human experiences that it cannot physically undergo, the virtual influencer exploits consumer vulnerabilities through manufactured, data-optimized trust. Because the CPA and CCPA frameworks do not explicitly compel the disclosure of a persona's *non-human nature* focusing instead only on disclosing *commercial relationships* the current Indian legal regime remains ill-equipped to police the deceptive mechanics of synthetic marketing.

ASCI GUIDELINES AND THE REGULATORY GAP

OVERVIEW OF ASCI INFLUENCER GUIDELINES AND DISCLOSURE REQUIREMENTS

The **Advertising Standards Council of India (ASCI)** serves as the voluntary self-regulatory body governing advertising content across the domestic digital ecosystem. Recognizing the exponential expansion of social-media-driven commerce, ASCI instituted the *Guidelines for Influencer Advertising on Digital Media* to protect consumers from covert marketing practices. The guidelines impose explicit **sponsored content rules**, dictating that any individual who has a "material connection" with a deploying brand must display a clear and prominent disclosure label.

Acceptable disclosure markers under the code include specific tags such as #ad, #sponsored, #partnership, or #collab. ASCI mandates that these disclosures must be positioned upfront—rendering them visible without requiring a user to click "see more" or scroll down—and must be maintained across all digital media formats, including ephemeral stories, video streams, and static posts.¹³

APPLICABILITY TO VIRTUAL INFLUENCERS

In an attempt to keep pace with emerging technology, ASCI expanded its framework to address synthetic media, stating that a virtual influencer must additionally disclose to consumers that they are not interacting with a real human being (Ciani, 2025). This specific clause mandates that the non-human disclosure must be upfront and prominent (Ciani, 2025).

Despite this progressive textual inclusion, structural problems of non-disclosure persist. Because ASCI operates fundamentally as a self-regulatory organization rather than a statutory body, its guidelines lack executive punitive mechanisms. While it can flag non-compliant profiles and request modifications, it cannot levy statutory financial penalties or initiate criminal prosecution for persistent non-compliance. This structural limitation transforms what should be strict consumer protection enforcement into a largely voluntary industry practice.

THE TRANSPARENCY GAP AND SUGGESTED REFORMS

To bridge this regulatory gap, transparency must transition from a voluntary industry code into a hard legal requirement integrated directly into India's consumer protection statutes. It is insufficient to merely disclose a *commercial link*; the law must mandate the disclosure of the endorser's *ontological status* (its state of being a non-human simulation).¹⁴

¹³ *Shiromani Gurdwara Prabandhak Committee v. Som Nath Dass*, (2000) 3 SCC 146 (India).

¹⁴ Advertising Standards Council of India, *Guidelines for Influencer Advertising in Digital Media* (2021).

This paper suggests amending the CCPA Guidelines to enforce the mandatory inclusion of standardized, visually distinct, unalterable text watermarks and spoken disclaimers across all promotional formats. These disclosures must utilize precise, unambiguous statutory nomenclature:

- **"AI Generated"**: To be deployed when the content, speech patterns, or visual assets are constructed autonomously via generative algorithms.
- **"Virtual Influencer"**: To be applied as a permanent profile tag and post header for any digital persona lacking an organic human substrate.
- **"Synthetic Personality"**: To be mandated for hybrid, brand-owned, or metaverse-native avatars that simulate human social presence for commercial persuasion.

Codifying these specific markers into federal consumer law ensures that the right to informed consent in the digital marketplace is preserved, preventing the sophisticated mechanics of synthetic authenticity from degenerating into legal consumer deception.

MEDIA ETHICS AND SOCIETAL CONCERNS

The proliferation of virtual influencers introduces profound ethical complexities to the media landscape, threatening to amplify deep-seated societal harms while operating in a largely unregulated legal environment. At the core of these ethical concerns is the perpetuation of unrealistic beauty standards and its direct impact on mental health. Unlike human creators who possess physical irregularities, virtual influencers are engineered to exist in a permanent state of aesthetic perfection, presenting mathematically flawless skin textures, symmetry, and proportions (Kondekar, 2025). Exposure to these unattainable digital ideals significantly exacerbates body dissatisfaction, social appearance anxiety, and identity vulnerabilities (Bharti, 2026; Mironica et al., 2024).¹⁵

This structural manipulation extends to the strategic exploitation of consumer emotions. By utilizing machine learning pipelines to analyze user sentiment, these synthetic personalities deploy optimized algorithmic narratives to foster intense, asymmetric parasocial relationships. This calculated intimacy poses severe developmental risks to children and young adolescents, whose developing self-concept and cognitive defenses are structurally unequipped to

¹⁵ Andreea Mironica et al., *Social Media Influence on Body Image and Cosmetic Surgery Considerations: A Systematic Review*, 16 Cureus e65626 (2024).

differentiate between human emotional reciprocity and automated marketing strategies (Liu et al., 2024).

Furthermore, virtual influencers frequently entrench regressive gender representation issues, as corporate developers often default to hyper-sexualized or highly stereotyped racial and gendered tropes to maximize click-through metrics and commercial traction. This systemic reinforcement of biased norms is further compounded by the imminent risk of deepfake integration.

The Ethical Imbalance: Because virtual entities are entirely malleable software assets, their underlying technology can be hijacked to generate unverified commercial claims, simulate deceptive behavioral modifications, or blend seamlessly into malicious deepfake architecture without triggering standard professional liability metrics.¹⁶

By decoupling mass media persuasion from human legal and moral agency, synthetic personalities operate as highly optimized vectors for behavioral engineering, outpacing India's anthropocentric consumer and media frameworks.

THE PROBLEM OF LEGAL PERSONALITY AND ACCOUNTABILITY

THE CONCEPT OF LEGAL PERSONHOOD AND ARTIFICIAL INTELLIGENCE

The fundamental architecture of liability under modern jurisprudence rests entirely upon the concept of **legal personhood**—the statutory recognition of an entity as a bearer of legal rights and duties. Historically, courts have divided the global legal landscape into two primary categories of persons: **natural persons** (living human beings) and **juristic/artificial persons** (non-human entities, such as corporations, deities, or municipalities, given legal status by statutory fiction).

As AI-driven systems achieve operational autonomy, a critical regulatory debate has emerged over whether AI entities can possess independent legal rights. In India, this boundary remains strictly human-centric. For instance, the Indian Patent Office definitively rejected the recognition of an autonomous AI system (*DABUS*) as a "true and first inventor," affirming that intellectual and legal agency under current statutory frameworks requires a cognizable natural or juristic persona.

¹⁶ *Shiromani Gurdwara Prabandhak Committee v. Som Nath Dass*, (2000) 3 SCC 146 (India); see also Indian Patent Office, *Dr. Stephen L. Thaler v. Controller General of Patents, Designs & Trade Marks*, Patent Application No. 202017019068 (2026).

THE ACCOUNTABILITY GAP IN SYNTHETIC MEDIA

Because virtual influencers lack juristic personality, they occupy a troubling legal vacuum. These synthetic personalities exercise immense socio-commercial influence, yet they operate entirely without legal responsibility. When a human influencer makes false claims, they face direct statutory civil and financial penalties under the Consumer Protection Act, 2019. Conversely, a virtual influencer can distort the digital marketplace with complete legal immunity.

This structural mismatch creates a profound **accountability gap**. When misleading or aggressive commercial behavior occurs, the legal fiction of the "persona" cannot be penalized; instead, the liability framework fractures. It scatters across an opaque, multi-layered back-end comprising software developers, creative agencies, and deploying brand owners, making traditional enforcement exceptionally difficult.

COMPARATIVE ANALYSIS OF LEGAL MODALITIES

To understand how virtual influencers evade the traditional mechanics of legal enforcement, it is essential to contrast them with recognized legal actors:¹⁷

Attribute	Natural Persons	Corporations	AI / Virtual Influencers
Source of Status	Biological birth and natural existence.	Statutory creation via legal incorporation.	None; operates as code and digital imagery.
Moral Agency	Complete individual consciousness and moral choice.	Aggregated human intent regulated by corporate boards.	Simulated agency governed by mathematical algorithms.

¹⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), art. 50, 2024 O.J. (L 1689).

Attribute	Natural Persons	Corporations	AI / Virtual Influencers
Capacity to Sue	Direct standing to initiate or defend legal actions.	Authorized to sue or be sued under corporate name.	Lacks independent standing; cannot be named a party.
Asset Ownership	Can legally own property and execute contracts.	Holds independent corporate property and capital.	Incapable of asset holding or execution of legal deeds.
Punitive Recourse	Subject to personal fines, bans, or incarceration.	Vulnerable to asset freezes, liquidations, and fines.	Immune; profiles can be deleted and instantly replaced.

THE JURISPRUDENTIAL FRICTION:

Corporations possess juristic personhood because they are bound by formal, registrable corporate governance structures and identifiable human shareholders. Virtual influencers, however, deploy anthropomorphic traits to look like natural persons while enjoying the complete absence of corporate or physical liability metrics.

By decoupling the act of commercial persuasion from any form of natural or legal personhood, synthetic personalities act as highly optimized vectors for corporate gain. They allow deploying brands to exploit consumer trust while leaving regulatory authorities with a "paper tiger" framework that has no viable legal subject to penalize.

WHO SHOULD BE RESPONSIBLE? DEVELOPING AN ALGORITHMIC ENDORSER LIABILITY MODEL

The Fragmented Liability Ecosystem

When an autonomous or semi-autonomous AI personality disseminates a misleading advertisement, assigning blame across a multi-layered back-end architecture creates significant legal uncertainty. Traditional tort and product liability models are structurally inadequate for generative systems. This is because they frequently attempt to isolate a single point of failure—

such as a developer bug—while ignoring the cooperative, multi-actor nature of synthetic media deployment.

Determining accountability requires dissecting the specific inputs of the four principal entities controlling the digital persona:

- **The AI Developers:** Software engineers often claim that "black-box" algorithmic emergence shields them from liability, arguing the system behaved independently of its initial code. However, developers must bear fault-based liability if they fail to implement scientifically validated safety standards, source training data unethically, or program the system to deliberately bypass disclosure guardrails.
- **The Deploying Brands:** As the primary economic beneficiaries of the synthetic persona, corporate brands cannot circumvent consumer protection standards by hiding behind an automated intermediary. Brands exercise ultimate administrative veto power over the campaign's direction, making them prime candidates for strict vicarious liability.
- **The Advertising Agencies:** Marketing intermediaries design the prompts, strategic narratives, and aesthetic contexts that give the virtual influencer its social influence. When an agency inputs specific instructions that generate deceptive visual or textual claims, it acts as a conscious legal director of the infringement.
- **The Social Media Platforms:** Hosting platforms maintain the distribution infrastructure and algorithmic amplification loops that deliver synthetic content to consumers. While protected by standard intermediary safe-harbor clauses, platforms face liability if they fail to enforce standardized content flagging or profit from un-watermarked AI advertisements.

THE ALGORITHMIC ENDORSER LIABILITY FRAMEWORK

The Conceptual Shift: To resolve this enforcement gridlock, this paper introduces the framework of "**Algorithmic Endorser Liability**." This model shifts the focus of consumer law away from trying to regulate the autonomous algorithm itself, instead tracing and penalizing the specific human and corporate entities that control and profit from the AI system.

This joint and proportionate liability model recognizes that complex technologies cause damage through shared human actions rather than isolated events. The core legal argument is straightforward: **the law must regulate the controller, not the algorithm.**

Under this framework, liability overlaps based on each entity's degree of commercial benefit and operational control. If a virtual influencer violates the Consumer Protection Act by making false product claims, a statutory presumption of joint liability is established. To escape civil penalties, back-end actors must actively prove they fulfilled their respective fiduciary duties of care—such as conducting independent algorithmic audits, verifying prompt safety, or executing transparent identity disclosures. This architecture ensures that as marketing automation grows, consumer protection remains tied to clear human accountability.

COMPARATIVE REGULATORY APPROACHES

Global Legislative Trajectories

As nations grapple with the legal vacuum surrounding synthetic personas, distinct regulatory philosophies have emerged across major jurisdictions. These frameworks offer vital structural lessons for the Indian digital ecosystem.

1. THE EUROPEAN UNION

The European Union's **AI Act** establishes a comprehensive, risk-based legislative blueprint. Under Article 50 of the Act, explicit **transparency obligations** dictate that providers must design interactive AI systems—including virtual influencers—so that users are informed upfront that they are engaging with artificial entities. Furthermore, providers of generative pipelines must ensure all synthetic video, audio, and textual outputs are marked in a permanently embedded, machine-readable format. Non-compliance risks severe administrative fines of up to €15 million or 3% of global annual turnover, prioritizing strict, preventative consumer disclosure.

2. THE UNITED STATES

The United States addresses synthetic marketing by extending traditional consumer protection enforcement through the **Federal Trade Commission (FTC) Endorsement Guides**. Rather than introducing standalone AI legislation, the FTC treats virtual influencers under its existing deception framework. Under these rules, if an AI entity simulates personal product experiences or masks its corporate-controlled nature, the FTC imposes direct civil liability on the deploying

brands and creative agencies. The focus rests heavily on correcting post-market consumer harm and commercial fraud.¹⁸

3. CHINA

China enforces some of the world’s most prescriptive, state-driven regulations via the Cyberspace Administration of China’s (CAC) **Labeling Measures for Content Generated by Artificial Intelligence**. These mandatory AI disclosure laws require creators and platforms to append unmistakable text watermarks (such as "AI-generated") at the beginning or end of text streams. For audio-visual assets, they require spoken disclaimers read at normal conversational speeds. Additionally, the rules mandate that platforms verify the professional credentials of influencers discussing regulated sectors like law or health, maintaining strict government control over algorithmic provenance.

4. THE UNITED KINGDOM

The United Kingdom maintains a decentralized, pro-innovation approach through its **AI governance initiatives**. Rather than passing a cross-sector statutory act, the UK empowers existing regulatory bodies—such as the Advertising Standards Authority (ASA) and the Competition and Markets Authority (CMA)—to interpret existing consumer and fair-trading laws flexibly against synthetic actors.

COMPARATIVE MATRIX AND LESSONS FOR INDIA

India's current regulatory posture remains highly fragmented. While ASCI outlines disclosure suggestions, it lacks statutory enforceability, and the Consumer Protection Act, 2019 lacks explicit provisions defining or penalizing non-human endorsers.

Jurisdiction	Primary Regulation	Mandatory AI Disclosure	Primary Liability Model
European Union	EU AI Act (2024)	Yes (Upfront + Machine-readable marking)	Risk-based (Ex-ante provider/deployer duties)

¹⁸ Federal Trade Commission, *Guides Concerning Use of Endorsements and Testimonials in Advertising*, 16 C.F.R. § 255 (2023).

Jurisdiction	Primary Regulation	Mandatory AI Disclosure	Primary Liability Model
United States	FTC Endorsement Guides	Limited (Required if omission deceives)	Consumer protection (Ex-post brand liability)
China	CAC AI Labeling Measures	Mandatory (Strict visual/vocal markers)	State-controlled (Platform & creator accountability)
United Kingdom	Sectoral Governance Initiatives	No (Case-by-case regulatory review)	Flexible enforcement (Empowered legacy regulators)
India	Consumer Protection Act, 2019	No Specific Law (Voluntary ASCI Code only)	Fragmented / Unclear liability chain

THE REGULATORY TAKEAWAY: India cannot afford to rely on a piecemeal, voluntary self-regulatory system to police synthetic media. To protect the domestic digital marketplace, Indian lawmakers should adopt a hybrid model: synthesizing the EU's strict *ex-ante* mandatory disclosure rules with the US model's sharp focus on corporate financial liability.

INDIA'S EMERGING AI GOVERNANCE FRAMEWORK

THE POLICY LANDSCAPE: NITI AAYOG AND STATUTORY PROPOSALS

India's overarching approach to artificial intelligence is shaped by the **National Strategy on Artificial Intelligence**, formulated by NITI Aayog. This strategic blueprint establishes a vision for socio-economic inclusion under the baseline ethos of #AIforAll. To govern the deployment of autonomous systems, NITI Aayog subsequently published its **Responsible AI Principles**, which delineate key ethical pillars: safety, reliability, inclusivity, privacy, and accountability.

In parallel, the Ministry of Electronics and Information Technology (MeitY) has pursued foundational legislative overhauls. The long-anticipated **Digital India Act (DIA) Proposals** are intended to succeed the aging Information Technology Act, 2000, establishing an expansive digital safety framework designed to tackle modern algorithmic challenges, including generative deepfakes, algorithmic bias, and intermediary responsibilities. This is complemented by the enforcement of the **Digital Personal Data Protection Act (DPDPA)**, which regulates consumer metadata processing, data minimization, and automated user profiling.¹⁹

THE INFLUENCER BLINDSPOT IN FEDERAL AI POLICY

The Structural Gap: Despite the rapid development of these cross-sector frameworks, India's emerging AI policies suffer from a critical blindspot: current federal legislative discussions completely ignore the regulation of virtual influencers and automated marketing personalities.

While macro-level policies extensively address existential technological threats, cybersecurity, and systemic data privacy, they treat commercial synthetic media as a marginal issue. For instance, the DIA proposals focus heavily on blocking political disinformation, deepfaked non-consensual pornography, and copyright infringements by large language models. However, they lack precise mechanisms to govern commercial actors who use generative AI to manipulate consumer behavior.

Similarly, the DPDPA protects against unauthorized user tracking, but it does not regulate how virtual personas use that data to target vulnerable demographics. By failing to integrate synthetic marketing into federal AI governance strategies, Indian lawmakers are leaving a multi-million-dollar digital market segment completely dependent on a voluntary self-regulatory system. This leaves consumers vulnerable to the complex, data-optimized tactics of synthetic authenticity.

TOWARDS A DEDICATED REGULATORY FRAMEWORK FOR VIRTUAL INFLUENCERS IN INDIA

The Three-Pillar Regulatory Model

To resolve the legal fragmentation governing synthetic marketing in India, this paper proposes a structured Three-Pillar Regulatory Model. This framework bridges the gap between the

¹⁹ Digital Personal Data Protection Act, No. 22 of 2023, India Code; Information Technology Act, No. 21 of 2000, § 79, India Code.

Ministry of Electronics and Information Technology (MeitY) and the Central Consumer Protection Authority (CCPA), shifting India's enforcement strategy from a reactive approach to clear statutory accountability.

PILLAR 1: STRUCTURAL TRANSPARENCY

The first pillar mandates strict **ex-ante identification** of all synthetic actors. Building upon the Advertising Standards Council of India's (ASCI) recent disclosure updates, the law must require two distinct forms of notification.

First, virtual personas must display a persistent, non-removable visual watermark reading "**AI Generated**" or "**Virtual Influencer**" across all visual frames. Second, for video and audio content, creators must include an explicit disclosure statement within the first ten seconds of the broadcast. These identity requirements must apply in tandem with standard sponsored content disclosures (#Ad or #Sponsored), ensuring consumers can immediately recognize both the commercial relationship and the synthetic nature of the persona.

PILLAR 2: ALGORITHMIC ACCOUNTABILITY

The second pillar establishes clear liability by implementing the **Algorithmic Endorser Liability** model. Because digital avatars lack independent juristic personhood, the law must target the entities that control them.

[Regulatory Oversight Board]

|

|—> Mandates Registration (Unique Virtual Registries)

|—> Enforces Transparency Audits (Code & Bias Reviews)

|—> Directs Complaint Mechanisms (CCPA Arbitrations)

To enable effective enforcement, this paper proposes mandatory **registration requirements** with MeitY for any commercial virtual influencer operating within India that crosses a designated follower threshold. Registered personas will be issued a unique digital identification token tied directly to an accountable legal entity—whether a corporate brand, an advertising agency, or a software development house. This registration layer is reinforced by periodic **transparency audits**, requiring corporate controllers to submit their underlying engagement

algorithms and text-prompt histories for independent review to detect manipulative consumer tracking or hidden behavioral optimization.

PILLAR 3: CONSUMER PROTECTION

The final pillar introduces dedicated safety mechanisms to insulate vulnerable demographics, particularly children, from automated persuasion. Because minors are highly susceptible to data-optimized parasocial bonds, the framework mandates strict **age-gating protocols** and explicitly bans virtual influencers from deploying hyper-personalized, real-time interactive loops on child-directed platforms.

Furthermore, this pillar institutes an automated **consumer complaint mechanism** integrated into the national consumer helpline, allowing users to report unlabeled synthetic promotions directly to the CCPA. Finally, the framework establishes strict **platform accountability**. Social media intermediaries will lose their statutory safe-harbor protections under Section 79 of the Information Technology Act if they fail to implement automated scanning systems to flag, demote, or remove non-compliant, un-watermarked synthetic advertisements.

The Jurisprudential Objective: By unifying these three pillars under an **independent regulatory oversight board**, India can move past temporary self-regulatory codes. This approach will establish a legally binding baseline of algorithmic honesty, ensuring the domestic digital economy remains fair, transparent, and safe for consumers.

CONCLUSION: FROM HUMAN INFLUENCE TO ALGORITHMIC INFLUENCE

SUMMARY OF FINDINGS AND REGULATORY GAPS

The ascension of virtual influencers within the Indian digital market marks a profound paradigm shift in the architecture of commercial persuasion, transitioning the creator economy from human influence to algorithmic influence. This legal analysis reveals a stark disconnect between the rapid technological deployment of synthetic personas and the anthropocentric statutes designed to regulate them.

While entities like Kyra and Naina Avtr successfully execute high-value brand campaigns, they do so from within a severe legal vacuum. The primary regulatory gaps identified stem from the foundational assumption of "human agency" embedded in the Consumer Protection Act, 2019, and the CCPA Guidelines, 2022.

Because an AI personality lacks juristic personhood, it cannot possess genuine opinions, execute statutory due diligence, or be sued for deceptive trade practices. Yet, these programmable advertising systems generate a highly optimized "Synthetic Authenticity"—using machine learning feedback loops and fabricated narratives to cultivate deep parasocial trust, manipulate consumer emotions, and project unrealistic standards without facing any direct legal responsibility.

RECOMMENDATIONS FOR INDIAN POLICYMAKERS

To preserve market integrity and insulate vulnerable demographics like children from covert manipulation, transparency must transition from a voluntary practice into a strict statutory command. Indian policymakers must recognize that traditional influencer regulations are fundamentally ill-equipped to govern automated marketing systems. Moving forward, the state must implement a dedicated legal framework built upon two structural interventions:

- **Mandatory Ontological Disclosure:** Amending federal consumer laws to compel the permanent display of standardized, machine-readable visual watermarks and audio disclaimers (e.g., "AI Generated" or "Virtual Influencer") across all promotional formats.
- **Codification of Algorithmic Endorser Liability:** Establishing a joint and vicarious liability regime that traces accountability past the autonomous software layer. Legal responsibility must be attributed directly to the human and corporate actors—developers, advertising agencies, and brand owners—who orchestrate, fund, and profit from the synthetic system.

Furthermore, social media platforms must be legally obligated to enforce automated scanning and provenance tracking. Intermediaries should face the automatic forfeiture of safe-harbor immunities under Section 79 of the Information Technology Act if they actively host or algorithmically amplify non-compliant, un-watermarked synthetic advertisements.

THE FUTURE OF VIRTUAL INFLUENCERS IN INDIA

Virtual influencers represent a fundamental shift in digital communication. While they offer significant commercial opportunities, they also challenge core assumptions underlying consumer protection and media regulation. India must move beyond traditional influencer regulation and develop a dedicated framework that recognizes AI-generated personalities as a

new category of market actor. The future of advertising may be artificial, but accountability must remain firmly human.

As generative AI pipelines evolve toward rendering fully autonomous, real-time interactive avatars within spatial environments, the pressure on India's regulatory borders will only intensify. If left unchecked, the commercial deployment of synthetic media risks decoupling consumer trust from market reality entirely. By establishing a dedicated, three-pillar governance model that champions automated disclosure and algorithmic liability, India has the unique opportunity to pioneer a balanced digital ecosystem—one that embraces technological innovation without sacrificing consumer rights.