

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Digital Identity in the Metaverse: Navigating Privacy, Data Protection, and the Evolving Legal Landscape

KIRTIKA SAHU* AND DR. RAKESH KUMAR PANDEY**

ABSTRACT

The proliferation of the metaverse as a persistent, immersive, and shared virtual ecosystem has fundamentally destabilised the ontological boundaries between physical and digital spaces, precipitating a paradigm shift in the conceptualisation of digital identity. As these virtual environments scale in complexity, establishing an effective regulatory architecture for identity governance introduces profound legal and technical friction. This paper provides a rigorous analysis of the evolving governance paradigms and regulatory lacunae surrounding digital identity within the Indian legal landscape, centring on the imperatives of user-conduct regulation, algorithmic content moderation, and systemic legal enforcement in Web3 spaces.

This paper posits that data privacy and protection mechanisms are foundational to secure identity management. Because the metaverse relies on the continuous harvesting and cloud-based storage of high-fidelity user data, including spatial analytics, behavioural profiling, and biometric inputs, digital identities remain uniquely vulnerable to unauthorised extraction, data asymmetry, and commercial exploitation. A failure to institute robust data-protection frameworks not only undermines fundamental privacy rights but amplifies the risk of identity-related cybercrimes, including synthetic identity fraud and virtual harassment. This study further addresses the challenges of cross-border jurisdictional enforcement inherent in decentralised virtual environments. Ultimately, it evaluates the efficacy of India's current statutory framework, specifically the Digital Personal Data Protection (DPDP) Act and the Information Technology Rules, to offer a comprehensive, forward-looking assessment of the legal implications shaping virtual-identity jurisprudence.

Keywords: *Digital Identity Governance, Metaverse Jurisprudence, Biometric Data Protection, Jurisdictional Friction.*

* Author is a Research Scholar at C.S.J.M. University, Kanpur, Uttar Pradesh, India.

** Author is a Professor at Department of Law, V.S.S.D. College, Kanpur, Uttar Pradesh, India.

I. INTRODUCTION

With the rapid growth of the technological era and the Internet of Things (IoT), the term metaverse has gained a prominent role in society. The term is not new; its history can be traced to 1992, when the American science-fiction writer Neal Stephenson coined it in his novel *Snow Crash*, which depicts a dystopian future in which the wealthy escape into an alternative, three-dimensional connected reality. Many believe the metaverse to be a three-dimensional manifestation of the internet and an upgrade upon it. The metaverse consists of many digital environments that are open, shared, and persistent, permitting users to access a wide range of experiences and services.¹ To give themselves a sense of presence, users can enter as digital avatars enhanced by Virtual Reality (VR) and Augmented Reality (AR) technology. In addition to an assurance of data continuity regarding identity, communications, transactions, and asset ownership, users may interact with one another. Contrary to what many believe, the internet would not be supplanted by the metaverse.² As the metaverse proliferates across the internet, it will inevitably alter user experiences. Not long ago, few had considered the metaverse; it is now one of the most talked-about technological concepts. The Steven Spielberg film *Ready Player One* offers one illustration of how people might escape the horrors of a dystopian future. A theme common to all accounts of the metaverse's history is the connection between virtual reality and the metaverse, which may be a beneficial instrument for helping individuals discover new technological tools and experiences.³

Notable examples in the field of the metaverse include Roblox, Sandbox, Decentraland, and numerous other online platforms.⁴ With the aid of personalised digital avatars, these platforms permit users to explore virtual places and communicate with one another. The ability for users to create experiences and assets is one of the key features of how the metaverse works, and virtual currencies and tokens may be useful for verifying transactions and ownership. In brief, the metaverse is a virtual space that allows users to interact with people from all over the world in an online reality. By using virtual- and augmented-reality headsets and glasses, users can live, explore, and grow within this virtual world.⁵ It can encompass numerous facets of the modern world that encourage user participation, such as social networking, online gaming, and cryptocurrency.

¹ Paul Schiff Berman, *GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS* 65-82 (2012).

² Robert Chesney & Danielle Citron, *Deepfakes and the New Disinformation Vanguard*, *FOREIGN AFF.*, Sept.-Oct. 2019, at 102.

³ Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 *THEORETICAL INQUIRIES L.* 157 (2019).

⁴ Lee A. Bygrave, *DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS* 124 (2002).

⁵ Chris Reed et al., *What Law Applies to the Metaverse?*, 4 *STAN. J. BLOCKCHAIN L. & POL'Y* 33 (2023).

II. THE METAVERSE: HOW IT FUNCTIONS

The metaverse refers to a collection of interactive and fully immersive three-dimensional (3D) environments, protocols, and technologies that integrate virtual reality (VR) and augmented reality (AR) to create a spatial framework for online interactions.⁶ It makes use of blockchain technology to facilitate social media, token economies, decentralised gaming platforms, and virtual land sales, and is sometimes referred to as the internet's future. Although still a relatively new idea, some of the most prominent technology businesses, including Microsoft, Apple, Google, and Meta (formerly Facebook), are competing to develop the technologies required to generate metaverse offerings. In the future, this virtual platform might serve as the venue for some regular online interactions; for instance, a user could play chess against an opponent on a virtual island owned by that user. Users can represent themselves in virtual reality through avatars, and it will be possible to store in-game items, land, and avatars on the blockchain as NFTs. The metaverse can also help businesses take advantage of next-generation marketing opportunities and socially engaging workspaces.

To understand how it functions, it is necessary to understand the key technologies powering the metaverse. The first and foremost is blockchain technology.⁷ The majority of applications in the metaverse depend on the blockchain, which serves as their foundation and offers the decentralisation and transparency essential for the system to function. Blockchain technology facilitates the integration of various metaverse functions, including governance, digital collectability, value transfer, accessibility, interoperability, and the verification of digital ownership. It offers many advantages: by acting as a virtual ledger, it facilitates the creation of a record of transactions.⁸ The decentralised database in which a blockchain stores its data also lowers the possibility of malfunction. The technology gathers data and groups it into units known as blocks; when storage capacity is full, a block is closed and coupled with other filled blocks to generate the blockchain, a chain of data. Because the blocks are connected, the data is organised chronologically by default, permanently created and given a time stamp by this structure. Once a block is sealed, it cannot be changed, which is crucial in ensuring that there are no manipulations and that the metaverse remains transparent. Other technologies, such as

⁶ Primavera De Filippi & Aaron Wright, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE* 182 (2018).

⁷ Yannick Radi, *The Emergence of Virtual Personhood: Private Law and Avatars in the Age of Spatial Computing*, 31 *EUR. REV. PRIV. L.* 411 (2024).

⁸ Julie E. Cohen, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* 140-56 (2019).

cryptocurrency, AR and VR, and artificial intelligence, also play a significant role in the functioning of this virtual world.⁹

III. THE CONSTITUTIONAL MATRIX: THE RIGHT TO PRIVACY AND COGNITIVE LIBERTY

The structural transformation of data from static text to dynamic physiological telemetry fundamentally disrupts classical constitutional doctrines of privacy. The foundational constitutional right to privacy in India, as articulated by the Supreme Court in the landmark case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*, guarantees informational self-determination, bodily autonomy, and spatial privacy as intrinsic components of the right to life under Article 21.¹⁰ However, the *Puttaswamy* doctrine assumes a bifurcated world: a physical individual who possesses rights, and a digital trail of historical records that must be protected against state and non-state overreach.¹¹

The metaverse introduces an intermediary layer that shatters this dichotomy: the avatar. The avatar functions as a hybrid legal construct. On one hand, it is an extension of the user's physical personhood and an instrument for exercising fundamental freedoms, such as the right to free speech and expression under Article 19(1)(a) and the right to assemble peacefully under Article 19(1)(b) of the Constitution. On the other, it is a proprietary digital manifestation entirely owned, coded, and monitored by a private platform provider's infrastructure.¹²

When an immersive platform records every micro-expression and gesture of an avatar, it is simultaneously mapping the unvarnished psychological and biological profile of the physical user behind it. Consequently, architectural surveillance within virtual environments violates the core tenets of the *Puttaswamy* test (legitimate state interest, necessity, and proportionality) by processing data that bypasses conscious user control. This continuous data harvesting infringes not merely upon informational privacy, but directly upon **cognitive liberty**, the absolute protection of an individual's internal mental and psychological autonomy under the umbrella of Article 21.

⁹ Paul de Hert & Serge Gutwirth, *Privacy, Data Protection and Law Enforcement: Distinction with a Difference*, in *PRIVACY AND DATA PROTECTION IN COMPLEX DIGITAL NETWORKS* 71 (C. Joubert ed., 2021).

¹⁰ *Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

¹¹ *Id.* at 320-25.

¹² de Hert & Gutwirth, *supra* note 9, at 71.

IV. STATUTORY EVALUATION: THE DPDP ACT, 2023 AND REGULATORY LACUNAE

As India navigates this complex frontier, the primary statutory defence mechanism is the Digital Personal Data Protection (DPDP) Act, 2023.¹³ While the DPDP Act introduces a modern framework for data regulation, its conceptual architecture remains anchored to the traditional flat-web era, creating significant regulatory lacunae when applied to immersive ecosystems.

A. The Structural Definitions: Data Fiduciary and Data Principal

Under Section 2(j) of the DPDP Act, the individual to whom the personal data relates is defined as the “Data Principal,” while the entity determining the purpose and means of data processing is termed the “Data Fiduciary” under Section 2(i). In a closed-loop metaverse platform, such as Meta’s Horizon Worlds, the platform provider acts as a massive, monolithic Data Fiduciary.

In decentralised metaverses built on Web3 architectures, such as Decentraland, however, the determination of “purpose and means” becomes highly diffuse.¹⁴ When decentralised autonomous organisations (DAOs), smart contracts, and independent third-party virtual-land developers share data-processing responsibilities simultaneously, isolating a single Data Fiduciary to bear civil liability and statutory penalties becomes practically impossible under the current text of the Act.¹⁵

B. The Breakdown of Notice and Consent Mechanics

Sections 5 and 6 of the DPDP Act establish that any processing of personal data must be preceded or accompanied by a clear, granular notice and must be based on explicit, unambiguous, and unconditional consent.¹⁶ This notice-and-consent framework becomes unworkable in an active metaverse environment for two distinct reasons.

Consent fatigue and spatial interruption. Forcing a user to read a privacy notice and provide affirmative consent every time their avatar steps into a new virtual zone, interacts with a different non-player character (NPC), or triggers an eye-tracking sensor would render the immersive experience unusable.

The involuntary nature of immersive data. Biometric and kinematic tracking is a technical operational requirement for spatial rendering. A user cannot withhold consent for eye-tracking or posture tracking while continuing to use the hardware; the processing is structurally

¹³ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

¹⁴ De Filippi & Wright, *supra* note 6, at 150-68.

¹⁵ Wessel Reijers et al., *Nowhere to Hide: Accountability and Governance Failure in Decentralized Autonomous Organizations*, 30 PHIL. & TECH. 291 (2021).

¹⁶ The Digital Personal Data Protection Act, *supra* note 13, §§ 5-6.

inseparable from the service itself, turning consent into an illusory “take-it-or-leave-it” contract and directly violating the requirement under Section 6(1) that consent be “free.”¹⁷

C. The Categorisation Deficit: Omission of Sensitive Personal Data

Unlike the European Union’s General Data Protection Regulation (GDPR), or India’s earlier Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which explicitly categorised biometric and health data as “sensitive personal data” requiring heightened regulatory protection, the DPDP Act omits any tiered classification of personal data, treating all personal data under a single, undifferentiated standard.¹⁸ Within spatial computing, the distinction between general personal data (for example, an email address) and deeply intimate biological data (for example, real-time heart-rate variation and saccadic eye movements) is entirely erased. By failing to afford enhanced statutory protection to biometric and physiological streams, the DPDP Act permits metaverse developers to process deep bodily telemetry under the same compliance thresholds used for basic web forms, provided general consent is acquired.¹⁹ This leaves Indian citizens vulnerable to unprecedented profiling without the safeguards of heightened judicial scrutiny or strict legislative thresholds.

D. Significant Data Fiduciaries and Algorithmic Compliance

Section 10 of the DPDP Act empowers the Central Government to designate certain entities as “Significant Data Fiduciaries” (SDFs) based on the volume and sensitivity of the data processed, the risks to the rights of Data Principals, and the implications for public order. Metaverse platforms, by virtue of their deep psychological data harvesting and high-risk profile, naturally cross into SDF territory. Once so designated, a platform is legally mandated under Section 10(2) to appoint an India-based Data Protection Officer (DPO), to retain an independent data auditor to conduct regular compliance assessments, and to undertake comprehensive Data Protection Impact Assessments (DPIAs). While these provisions offer a valuable regulatory hook for state oversight, their efficacy hinges entirely on the forthcoming DPDP Rules.²⁰ Traditional data-auditing practices are ill-equipped to audit the real-time neural streams,

¹⁷ Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

¹⁸ *Data Privacy in India: A Critical Analysis of the Digital Personal Data Protection Act, 2023*, REC. OF L. (May 2026), <https://recordoflaw.in/data-privacy-in-india-a-critical-analysis-of-the-digital-personal-data-protection-act-2023/>.

¹⁹ TATA CONSULTANCY SERVS., *Mitigating Risks for Effective User Privacy Protection in Metaverse Experience* 12-15 (TCS Rsch. White Paper, 2025).

²⁰ MINISTRY OF ELECTRONICS & INFO. TECH., *Draft Digital Personal Data Protection Rules* (Gov’t of India Gazette Notification, 2025-26).

immersive edge-computing architectures, and algorithmic profiling engines native to virtual spaces.

V. LEGAL CHALLENGES

The world of today has seen a rapid increase in technology, which has provided access to the metaverse, a virtual reality built mainly on blockchain technology. With the help of an avatar, users can engage in activities that are not possible in reality. Companies involved in the metaverse tend to violate individuals' privacy by collecting personal data such as voice recognition and fingerprints. The principal legal challenges are examined below.²¹

A. Security

In the realm of the metaverse, security plays an important role, because, without reliability and security, no individual will spend time and money in a virtual environment. Security breaches persist and demand quick action to re-establish users' trust. As discussed in the earlier sections, blockchain technology has limited scope for safeguarding the data of individuals; a blockchain that is prone to exploitation or has an inadequate structure can cause problems, and smart contracts that are not carefully coded may allow breaches and pose additional risks.²² Finally, web users can still be deceived into divulging their passwords through traditional phishing scams and other strategies.

B. Privacy

The metaverse could substantially increase the amount of biometric data and personal information that technology companies gather about people. Features such as voice recognition and recordings enhance the immersive experience,²³ but they also raise significant privacy concerns. Additional measures intended to strengthen metaverse security, including voice activation, facial recognition, and eye recognition, make identity theft far more likely at this level of data collection.²⁴ Voice recordings from metaverse platforms could be used by criminals against victims, and it is possible to create bots that mimic real people. As with the ad-based economy of Web 2.0, behavioural data may be improperly managed and sold to interested parties.

²¹ Helen Nissenbaum, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 67-84 (2010).

²² DATA PRIVACY COMPLIANCE INST., *Identity Is the New Perimeter: Addressing Real-Time Behavioral Threat Vectors in Web3 Systems* (Privacy Day 2026 Summit Report, 2026).

²³ EUROPOL INNOVATION LAB, *The Next Tech Horizon: Criminal Vectors in Cross-Platform Spatial Ecosystems* 8 (2026 Threat Update, 2026).

²⁴ Graham Greenleaf, *ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES* 312 (2014).

C. Intellectual Property Rights and the Metaverse

Intellectual property rights and the metaverse are closely related. There is a widespread belief that the metaverse is an enigmatic place in which it becomes more crucial to distinguish between the real and virtual worlds. Created by combining augmented reality and virtual reality, it provides a universe full of possibilities.²⁵ Through virtual avatars, users can travel virtually, trade digital assets, and lead an “invented” life. This is where intellectual property rights come into the picture, to regulate the ownership of patents and copyrights.

The metaverse is a virtual extension of the physical world. In 2022, the shoemaker Nike filed a complaint against the online sneaker reseller StockX, alleging that an NFT it had released violated Nike’s trademark.²⁶ In January 2022, StockX unveiled its Vault NFT collection, in which every NFT was linked to a tangible product that the online merchant had already bought to resell on its website. Nike claimed that StockX infringed its intellectual property by minting NFTs connected to its trademark. According to StockX, because each NFT was linked to a genuine physical object, its service was identical to that of any other e-commerce vendor or marketplace that uses product photographs to offer goods; it also relied on the principle that, once a genuine product is lawfully sold, trademark rights are no longer attached to it, leaving the buyer free to continue selling the goods as it sees fit.²⁷

Technology firms are competing to develop novel metaverse products, the characteristics of which are powered by technologies such as virtual reality and machine intelligence. In this context, it is important to consider how these innovations might be patented.²⁸ The metaverse is a virtual world that is home to numerous innovations, and virtual reality will become increasingly significant, allowing many people to perform tasks in real time. Consequently, these issues need to be covered by the intellectual property laws currently in effect; sadly, India’s intellectual property laws lack such provisions. This opens the door to further technological advancement as the metaverse develops, and legislation addressing these issues must be enacted.²⁹

²⁵ Danielle Keats Citron, *FIGHT DARK DATA: CYBERSTALKING, AVATARS, AND THE INTIMATE PRIVACY CRISIS* 185-99 (2024).

²⁶ Meg Leta Jones, *The Right to Be Forgotten in the Metaverse: Erasure and Anonymization Challenges in Persistent Spatial Architecture*, 16 J. TECH. L. & POL’Y 22 (2025).

²⁷ *Rogers v. Grimaldi*, 875 F.2d 994 (2d Cir. 1989).

²⁸ Mayank Pandey, *IPR Challenges in the Metaverse*, 2 J. LEGAL RSCH. & JURIDICAL SCI. 10 (2023), <https://jlrjs.com/wp-content/uploads/2023/03/34.-Mayank-Pandey.pdf>.

²⁹ CENTRE FOR DEMOCRACY & RULE OF LAW, *The Avatar Paradox: Infringement of Personality Rights in Virtual Environments* 8 (Policy Brief, 2024).

VI. LEGAL CONCERNS REGARDING DATA PRIVACY AND PROTECTION

The first section of this paper addressed how the metaverse affects users' privacy. No law yet addresses the violation of data privacy and protection in the virtual environment of the metaverse, in which users provide details such as voice, fingerprint, and facial recognition data. The metaverse will surely bring new dimensions to the data-protection and privacy landscape. Where data-protection regulation has so far addressed physical data about people and their movement between countries, the virtual world creates new actors, namely avatars, alongside the original users, together with vast quantities of data generated from new sources, such as facial and eye expressions, as users move between different metaverses. This carries many complications, concerns, and policy issues for privacy and data protection.³⁰

This concept unveils a range of privacy and data-protection issues that put current regulatory frameworks to the test. First, it can be difficult to identify who is responsible for processing, storing, and protecting data, given the variety of roles within the metaverse and the way they overlap with the duties stipulated by data-protection laws. Because of its interconnectedness, there are questions regarding jurisdiction, portability, and the laws applicable to particular situations.³¹ The various data-collection methods used in the metaverse, such as eye-tracking and emotion-responsive technologies, make it difficult to obtain user consent and could unintentionally violate privacy. The sheer volume of data stored also raises the possibility of mass profiling, enabling decision-making, targeted advertising, and even state surveillance to be carried out using private information such as biometrics and emotional responses. Disinformation and sexual harassment are two examples of harmful and illegal content that must be regulated in the decentralised metaverse environment. The legal status of avatars calls into question the need for a legal personality distinct from users, and introduces risks to user identity and privacy. The widespread distribution of content via Web 3.0 and blockchain-based platforms makes it challenging to protect intellectual property rights, and, although Non-Fungible Tokens (NFTs) are touted as a solution, concerns persist about the applicable legal requirements and jurisdictions.³² Furthermore, the sharing of data for investigations calls for international treaties that balance security against privacy and data protection. In conclusion, the metaverse presents significant threats to a nation's digital sovereignty, raising issues concerning digital banks, citizenship, economies, currencies, and taxation. Its intricacies present

³⁰ Hedaia-T-Allah Nabil Abd Al Ghaffar, *Data Protection in the Metaverse: Concerns and Implications*, GLOBAL J'S, Vol. 23, No. 1, 2023, at 3, <https://globaljournals.org/item/2-Data-Protection.pdf>.

³¹ Viktor Mayer-Schönberger, *DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE* 114 (2009).

³² Margot E. Kaminski, *Regulating Real-World Surveillance*, 98 WASH. L. REV. 711 (2023).

a unique set of challenges that legislators and legal authorities must overcome, whether by modifying existing frameworks or creating new ones.

VII. CONCLUSION AND STRATEGIC RECOMMENDATIONS

In sum, the metaverse offers great potential, but it also brings considerable hazards and challenges, particularly in data protection, economics, society, and behaviour. The variety of sources influencing data collection, and the lack of clarity surrounding the legal identity of avatars, create obstacles at the data-generation stage. Challenges at the data-transfer stage include problems of interoperability and questions about data-transfer mechanisms between the metaverse and the real world. Threats of mass profiling and the spread of harmful and illicit content arise at the usage stage, while the data-sharing stage is complicated by the legal and investigative challenges surrounding data sharing between the two worlds. Many concerns also remain unresolved regarding data storage, archiving, and destruction, and there are serious threats to national data sovereignty.³³ It is critical that nations and the international community act proactively as the metaverse develops. Pre-emptive measures should be implemented before its extensive development, from the embryonic stage onward, to mitigate possible hazards and optimise its advantages. This proactive approach involves developing extensive legal frameworks, international agreements, and ethical standards that ensure responsible use, the protection of user rights, and data sovereignty.³⁴ Through the proactive resolution of these concerns, interested parties can shape the legal regime in a manner that promotes creativity and diversity while observing privacy and security.³⁵ In establishing a reliable user-authentication system, certain customised security techniques are required, including voice activation, fingerprints, eye and facial recognition, and other biometric information. It is essential that whatever data is collected through these techniques is stored and used scrupulously, and that sufficient data-protection mechanisms, supported by robust legal frameworks, are adopted to ensure security.

To steer this evolving landscape safely and to safeguard digital identity within India and the broader global community, the following multi-layered legal interventions are urgently required.

³³ Shoshana Zuboff, *Surveillance Capitalism and the Challenge of an Immersive Digital Order*, 15 J. CONSUMER AFF. 44 (2024).

³⁴ JUSTICE B.N. SRIKRISHNA COMM. OF EXPERTS, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 89 (Ministry of Electronics & Info. Tech., Gov't of India 2018).

³⁵ Cristiano de Azevedo, *Biometric Dark Patterns: Evaluating Real-Time Spatial Optimization and Neuromarketing Schemes Under Consumer Protection Acts*, 9 IMMERSIVE TECH. L. REV. 202 (2025).

Enact statutory tiering under the DPDP Rules. The Central Government must use its rule-making power to classify kinematic data, eye-tracking metrics, and physiological telemetry explicitly as high-risk personal data. Processing these streams must require mandatory Data Protection Impact Assessments (DPIAs) and explicit, time-bound, revocable consent isolated from general hardware-licensing terms.

Mandate privacy-by-design and edge processing. Regulatory bodies must impose privacy-by-design obligations on hardware manufacturers under consumer-protection frameworks. High-fidelity biometric data required for foveated rendering or kinetic translation must be processed locally, on the secure enclave of the user's headset device (edge computing). Only anonymised, aggregated, or localised vector coordinates should ever be transmitted to platform cloud servers.

Establish a legal-status framework for avatars. Indian jurisprudence must evolve to recognise the legal nexus between a physical human and their primary digital avatar. Unauthorised replication, biometric scraping, or modification of a user's unique identity avatar must be statutorily recognised as an actionable infringement of the right to personal identity and bodily integrity under Article 21.

Formulate an international convention on virtual governance. Because decentralised Web3 spaces defy geographic boundaries, India should lead multilateral diplomatic efforts to establish a unified international framework, a *Lex Digitalis Spatialis*, to standardise identity verification, manage cross-border digital evidence, and enforce privacy penalties against extraterritorial distributed networks.

The metaverse represents a profound leap in human connectivity, but its current structural trajectory poses an existential threat to individual privacy and identity security. The technical realities of spatial computing render traditional notice-and-consent mechanisms, flat data definitions, and state-bound jurisdictional rules obsolete. If left unguided by proactive, adaptive legal frameworks, the metaverse risks devolving into an unmitigated panopticon of biological and psychological surveillance.³⁶

³⁶ Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).