



LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.319>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

METaverse AND LAW: A COMPARATIVE STUDY OF THE LEGAL CHALLENGES IN THE VIRTUAL WORLD

Isha Rajput¹ & Aayushi Gupta²

I. ABSTRACT

The metaverse presents a complex legal challenge because immersive virtual environments combine identity, property, commerce, communication, and behavioural interaction in ways that India's existing cyber-law framework does not specifically address. This paper examines the absence of a metaverse-specific legal framework in India and evaluates whether the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, and existing intellectual-property and consumer-protection laws are sufficient to regulate metaverse-related harms. The study adopts a doctrinal and comparative legal methodology, relying on Indian and foreign statutes, case law, regulatory materials, and secondary literature. It compares India's position with regulatory and policy developments in the European Union, the United States, Japan, South Korea, and Pakistan. The comparative analysis shows that while the European Union has advanced platform-accountability and AI-governance models through instruments such as the Digital Services Act and AI Act, India's present framework remains comparatively fragmented. The Research Gap section identifies major deficiencies, including the absence of metaverse-specific legislation, weak platform accountability, lack of behavioural norms for avatar conduct, limited judicial engagement with virtual property, and insufficient international alignment. The Case Laws section further shows that Indian courts have begun addressing NFTs, personality rights, privacy, and digital assets, but issues such as avatar harassment, virtual land ownership, biometric exploitation in immersive spaces, and unfair platform terms remain largely untested. The paper concludes that India should adopt targeted amendments to the Information Technology Act, enact a Digital India Act responsive to metaverse-specific harms, and establish institutional reforms including a behavioural code, regulatory sandbox, multidisciplinary task

¹ 9th Semester B.Com LL.B. (Hons) student at Prestige Institute of Management and Research Gwalior (India). Email: rajputisha759@gmail.com

² 9th Semester BBA LL.B. (Hons) student at Prestige Institute of Management and Research Gwalior (India). Email: ir8835513@gmail.com

force, and stronger international cooperation.

II. KEYWORDS

Metaverse; Virtual Property; Personality Rights; Data Protection; Platform Accountability.

III. INTRODUCTION

The evolution of digital technology has transformed the manner in which individuals communicate, transact, work, learn, and participate in social life. The internet has not merely altered modes of entertainment and communication; it has reshaped social, commercial, professional, and governmental interactions. Contemporary technological development now points towards increasingly immersive cyber environments and advanced digital platforms.

One such development is the emergence of the “Metaverse,” which may be understood as an advanced stage of cyber technology combining elements of virtual reality, augmented reality, mixed reality, and interactive digital environments. The metaverse has emerged as one of the significant technological innovations of the twenty-first century, as it merges aspects of physical reality with immersive virtual spaces. It offers considerable possibilities for education, commerce, governance, entertainment, and social interaction. At the same time, it raises complex legal questions relating to jurisdiction, digital identity, virtual property, platform accountability, privacy, data protection, intellectual property, and criminal liability.

In India, the Information Technology Act, 2000 and the rules framed under it continue to form the principal foundation of cyber-law regulation. However, these instruments were primarily designed for conventional internet-based activities and do not expressly address the distinctive challenges created by immersive metaverse environments. The decision in Justice K.S. Puttaswamy (Retd.) v. Union of India affirmed privacy as a fundamental right and remains central to the protection of digital rights in India. Nevertheless, the case also illustrates the continuing need for legal frameworks capable of responding to emerging

technologies. In this context, issues of algorithmic governance, artificial intelligence regulation, and personal-data protection have acquired renewed importance, particularly after the enactment of the Digital Personal Data Protection Act, 2023.

Unlike the European Union, which has developed broader regulatory responses through instruments such as the Digital Services Act and the Artificial Intelligence Act, India does not yet possess a metaverse-specific legal framework. This regulatory gap raises serious concerns regarding user safety, liability, intellectual-property protection, digital autonomy, and the effective enforcement of rights in virtual environments.

Virtual land and other digital assets are increasingly being represented through non-fungible tokens, with individuals and organisations investing substantial value in metaverse-based property. This development raises several unresolved legal questions. It is unclear whether traditional land-law concepts can apply to virtual property, whether territorial rules can protect users against unauthorised interference with privately controlled virtual spaces, and whether virtual property can be mortgaged, transferred, inherited, or enforced as a legally protected asset. In addition, immersive digital environments may also be misused for unlawful marketplaces, fraud, harassment, impersonation, and other forms of cyber-enabled misconduct. These risks require careful consideration of the legal safeguards necessary to regulate harmful conduct within the metaverse.

A global regulatory institution for the metaverse may be desirable in principle, but its practical implementation would be difficult because of jurisdictional, technological, and enforcement-related limitations. Therefore, domestic legal reform, supported by international cooperation, becomes essential.

This paper argues that India must move beyond fragmented regulation by introducing targeted amendments to the Information Technology Act, 2000 and by formulating legal frameworks specifically tailored to immersive virtual ecosystems. It advocates an interdisciplinary approach that combines law, technology, policy, ethics, and institutional oversight to ensure accountability,

safeguard user rights, and build public trust. Ultimately, the study concludes that proactive legal innovation is necessary for India to navigate the evolving digital frontier and to transform the metaverse into a secure, accountable, and rights-protective virtual space.

A. Research Objectives

This paper seeks to:

1. Identify the specific gaps in India's current legal framework (including the IT Act, 2000, the Digital Personal Data Protection Act, 2023 and the Bharatiya Nyaya Sanhita, 2023) in addressing conduct in the metaverse.
2. Conduct a comparative analysis of the approaches taken by the European Union, the United States, Japan, South Korea and Pakistan to the regulation of virtual and immersive spaces.
3. Assess the sufficiency of current Indian statutory and case law in regulating metaverse harms (avatar harassment, virtual property disputes and data misuse); and
4. Recommend legislative, regulatory and institutional reforms that would allow India to effectively regulate the metaverse while ensuring user safety and innovation.

B. Research Questions

This paper seeks to answer:

1. What are the key gaps in India's existing legal framework in relation to jurisdiction, identity, data protection and virtual property in the metaverse?
2. How do the approaches of the European Union, the United States, Japan, South Korea and Pakistan compare to India's approach to metaverse regulation, and what lessons could India learn from them?
3. How far can India's current set of statutory and judicial tools be stretched to regulate metaverse-specific harms?
4. where do genuine regulatory gaps continue to exist?

5. What are the legislative, regulatory and institutional reforms that would best serve India's interests when regulating the metaverse?

C. Research Methodology

This paper adopts a doctrinal and comparative legal research methodology. Its sources include Indian and foreign statutes, delegated legislation, case law, secondary literature including academic commentary, regulatory advisories and policy reports.

Its comparative element compares the approaches of five jurisdictions the European Union, the United States, Japan, South Korea and Pakistan to the current and prospective regulation of the metaverse in light of India's existing and proposed legal framework.

This research is based exclusively on publicly available legal materials and does not involve empirical or fieldwork.

D. History

The history of virtual reality (VR) and the metaverse includes several key developments. It began in 1838 with Sir Charles Wheatstone's work on 3D images. then 1935 rolled in, Stanley Weinbaum wrote the short story named "Pygmalion's Spectacles," which imagined immersive experiences. Morton Heilig created the Sensorama in 1956, one of the first VR machines, which gives us a virtual effect and gives us experiences. In the late 1970s, MIT's Architecture Machine Group, under the direction of Andrew Lippman, developed the Aspen Movie Map, an early interactive system that allowed users to take virtual tours of Aspen, Colorado. The project began in 1978 and became operational through demonstrations in 1979.³

The term "metaverse" was first used by Neal Stephenson in his 1992 novel "Snow Crash," where it represented an escape from reality. "Second Life," launched in

³ Sources for this section include More Than Digital, History & Evolution of the Metaverse Concept, <https://morethandigital.info/en/history-evolution-of-metaverse-concept/> (last visited Aug. 26, 2026).

2003, let users interact and create in a virtual world. The release of "World of Warcraft" in 2004 showed the potential for online gaming. In 2010, Palmer Luckey developed the Oculus Rift, sparking new interest in VR. Facebook bought Oculus in 2014, marking a major investment in this technology.

The popular game "Pokémon GO," released in 2016, helped bring augmented reality to a wider audience. In 2021, Facebook changed its name to Meta, highlighting its focus on the metaverse. VR continues to evolve, becoming more accessible and user-friendly.

This trend is set to persist with annual releases of thinner high-resolution VR headsets with quicker hardware, reasonable battery life, and lower price points. As the metaverse is a combination of virtual world or virtual reality [VR], augmented reality [AR] or mixed reality, and hyperreality in which users can interact with the people by representing themselves as avatars in a 3D display, and can feel or sense, or experience, focused on social and economic connection.

Virtual reality (VR) is like stepping into a whole new world. It's all about diving into a digital universe that feels real. You put on a headset and jump into a made-up world; it could be a game, a class, or a virtual tour.⁴

Augmented reality⁵ (AR) is like overlaying digital content on top of what you see in real life, making it more interactive and engaging. Think of Pokémon GO or filters on your phone, your surroundings stay real, but with virtual enhancements.

Hyperreality⁶ is the concept where the fake stuff feels more real than the actual world. It's when digital stuff or media gets all mixed up, making it hard to tell what's real and what's made up, like being part of fake online characters or getting sucked into ads that feel like real life. for example, in fabricated online personas or advertising

⁴ Wikipedia, Virtual Reality, https://en.wikipedia.org/wiki/Virtual_reality (last visited Aug. 26, 2026).

⁵ Wikipedia, Augmented Reality, https://en.wikipedia.org/wiki/Augmented_reality (last visited Aug. 26, 2026).

⁶ Wikipedia, Hyperreality, <https://en.wikipedia.org/wiki/Hyperreality> (last visited Aug. 26, 2026).

designed to mimic lived experience.⁷

E. Literature Review

1. Summary of “Challenges in the Metaverse Jurisdiction and International Treaty Law”

R.R. Krishnaa’s article, “Challenges in the Metaverse Jurisdiction and International Treaty Law,” examines the difficulty of applying conventional legal principles to immersive digital environments shaped by virtual reality, augmented reality, blockchain-based systems, and platform-mediated interaction. The article’s central contribution lies in identifying how legal rules designed for territorially bounded, real-world transactions may become inadequate when applied to borderless virtual environments. The article specifically considers questions of jurisdiction, accountability, digital identity, virtual assets, and international cooperation in the metaverse.⁸

Krishnaa begins by treating the metaverse as an advanced digital service environment, but distinguishes it from ordinary online platforms because users may interact, transact, socialise, own virtual assets, and engage in conduct capable of producing legal consequences. This creates a threshold problem of legal responsibility: when harmful conduct occurs in a virtual space that is accessible across jurisdictions, it becomes difficult to determine which country’s law should apply, which court may exercise jurisdiction, and which entity should be responsible for enforcement.

The article identifies four principal legal concerns. First, jurisdictional confusion arises because metaverse interactions may occur across national borders without a clear territorial connection. Traditional jurisdictional doctrines may therefore be insufficient to regulate transactions, disputes, or offences committed within virtual

⁷ Jean Baudrillard, *Simulacra and Simulation* 1–2 (Sheila Faria Glaser trans., Univ. of Mich. Press 1994) (1981).

⁸ R.R. Krishnaa, *Challenges in the Metaverse Jurisdiction and International Treaty Law*, IRPJ (2023), <https://irpj.euclid.int/articles/challenges-in-the-metaverse-jurisdiction-and-international-treaty-law/> (last visited Aug. 26, 2026).

environments. Secondly, the article discusses emerging “meta-crimes,” including avatar impersonation, virtual harassment, bullying, deepfake-based misconduct, and other forms of identity-based harm that do not fit neatly within existing criminal-law categories. Thirdly, Krishnaa highlights data vulnerability, noting that metaverse platforms may collect extensive personal, behavioural, and biometric information, including patterns of movement, voice, visual interaction, and other immersive data points. In the absence of coordinated privacy standards, such data collection may increase risks of profiling, surveillance, manipulation, and non-consensual processing. Fourthly, the article identifies treaty gaps, particularly the limited capacity of existing cybercrime instruments to address virtual property, smart contracts, avatar-based identity, and immersive cross-border misconduct.

Krishnaa consequently argues for the development of an international legal framework capable of regulating metaverse activity while preserving innovation and ensuring accountability. The article is therefore relevant to the present paper because it supports the view that metaverse governance cannot depend exclusively on domestic cyber-law rules or existing international instruments. Instead, it requires coordinated legal standards addressing jurisdiction, identity, property, data protection, and enforcement in immersive digital environments.

2. Summary of “Identity, Crimes, and Law Enforcement in the Metaverse”⁹

The article “Identity, Crimes, and Law Enforcement in the Metaverse” examines the legal and ethical implications of immersive virtual environments, particularly in relation to identity, criminal conduct, and enforcement. Although the manuscript presently cites the article as a 2023 source, external verification indicates that the peer-reviewed version appears in *Humanities and Social Sciences Communications* as a 2025 publication. The article’s structure is directly relevant to this paper because it organises metaverse governance concerns around three

⁹ Identity, Crimes, and Law Enforcement in the Metaverse, *Humanities and Social Sciences Communications* (2023), <https://share.google/4xZW24FOYUE53y3XL> (last visited Aug. 26, 2026).

principal themes: identity, crimes, and law enforcement.

The article argues that identity in the metaverse cannot be reduced to a user's name or visual representation. Instead, identity may consist of multiple layers, including representational identity, data-based identity, and legally identifiable or biometric markers. Representational identity includes avatars, pseudonyms, behavioural expression, gestures, and other forms through which users present themselves in virtual spaces. Data-based identity consists of the digital traces generated through a user's conduct and interactions. Identification may also include legally relevant indicators such as official credentials, biometric information, voice patterns, or other markers capable of linking a virtual persona to a real person. These layers are significant because they affect questions of accountability, rights, liability, and punishment in cases involving impersonation, harassment, fraud, or avatar-based harm.

The article further distinguishes between existing cybercrimes and more complex metaverse-specific harms. Conventional cybercrimes may include identity theft, money laundering, fraud, unauthorised access, and virtual property theft. By contrast, immersive environments may also give rise to conduct that produces psychological or emotional harm without necessarily causing physical injury. Examples include avatar-based harassment, virtual sexual misconduct, non-consensual manipulation of digital identity, and the creation or misuse of unlawful or harmful virtual representations. The article therefore raises an important conceptual question: whether criminal law should recognise certain forms of virtual harm when the injury is primarily emotional, psychological, reputational, or identity-based rather than physical.

In relation to law enforcement, the article identifies jurisdictional fragmentation as a central challenge. Metaverse-related conduct may involve users, servers, platforms, and victims located in different countries, making investigation and prosecution difficult under ordinary territorial models. The authors therefore support stronger international cooperation, clearer legal definitions, and technologically assisted enforcement mechanisms, including appropriate use of

artificial intelligence and blockchain-based tools. At the same time, the article cautions against both excessive decentralisation and excessive centralised control. It favours a balanced governance model involving states, platform providers, enforcement agencies, and users.

The article also contributes to the ethical dimension of metaverse regulation by considering difficult questions concerning AI avatars, harmful simulations, platform moderation, and culturally sensitive content. Its relevance to the present paper lies in showing that metaverse regulation requires more than protection of digital images or assets; it also requires legal recognition of the user's autonomy, dignity, safety, and identity within immersive virtual environments.

F. Research Gap

1. No Metaverse-Specific Law

India also relies on traditional legislation like the IT Act (2000) and DPDP Act (2023), and they were not designed for immersive environments. There is no acknowledgement of avatar personality, intellectual property within the virtual universe, or smart contracts.

Although the Digital Personal Data Protection Rules, 2025 introduce obligations relating to consent managers, data fiduciaries, and data protection compliance, they do not specifically address the collection and processing of biometric and behavioural data generated within metaverse platforms. This continues to create a regulatory gap for immersive digital environments.

2. Weak Platform Accountability

India's platform-accountability framework has developed beyond the position that there are no regulatory directives at all. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and brought into force on 20 February 2026, specifically strengthen intermediary due-diligence obligations in relation to AI-generated and synthetically generated information, including deepfakes and other manipulated audio, visual, or audio-visual content. These Rules are directly

relevant to metaverse-related concerns such as avatar impersonation, synthetic identity manipulation, deepfake-based harassment, and other forms of “meta-crime.”

However, while the 2026 Rules narrow the platform-accountability gap, they do not fully close it. India still lacks a comprehensive metaverse-specific regime comparable to the European Union’s Digital Services Act in relation to systemic risk assessment, platform transparency, user redress, immersive-space moderation, and adjudication of disputes arising within virtual environments. Therefore, the gap should be understood not as a complete absence of platform regulation, but as the absence of a dedicated and comprehensive framework for platform accountability in the metaverse.

3. No Moral Codes for Cyber Conduct or Virtual Behavior

Only South Korea has released behavioral codes for avatars and immersive behavior. There is no legislation in India to cover harassment, impersonation, and emotional distress in virtual spaces.

4. Limited Judicial Engagement

Indian courts are now facing a vast number of cases centered around NFTs and blockchain, with no established jurisprudence and no regulatory certainty regarding the treatment of digital assets.

5. No Harmonization/ lack of international alignment

India has neither taken nor signed any global treaty initiative on regulating the Metaverse and is thus susceptible and likely liable to cross-jurisdictional legal showdowns and enforcement vacuums.

6. The BNS/BNSS Transition and Its Limits

The Bharatiya Nyaya Sanhita, 2023 will replace the Indian Penal Code from 1 July 2024 and update a number of sections relating to cyber offences, including those relating to identity theft, cyberstalking and electronic impersonation. While the Sanhita did not anticipate avatar-based conduct when drafting its provisions, it remains to be seen whether the provisions can be forcibly extended to avatar harassment, virtual

impersonation or even deepfake "meta-crimes" without explicit revision.

A paper arguing that traditional criminal law is not prepared to deal with metaverse-specific harms would need to consider India's existing criminal statute (and not the pre-2024 code alone); even within the BNS framework, there are gaps in regard to virtual conduct that causes neither physical nor direct financial damage.

IV. COMPARATIVE STUDY OF GLOBAL APPROACHES

A. The European Union

The European Union doesn't have a single metaverse law regulation; however, a set of existing regulatory frameworks and is making regulatory proposals to address existing and potential risks in the immersive virtual world.

1. Key Legal Provisions & Approaches (European union)

- They have a powerful, robust framework, like (General Data Protection Regulation)¹⁰, which protects biometric and behavioral data
- Platform accountability and content moderation are enforced (Digital Services Act)
- AI risk governance specifies classes of AI systems by risk level (AI Act)¹¹

2. India: Comparative Status & Gap

- India's Digital Personal Data Protection Act, 2023 ¹²provides a domestic data protection framework, but lacks a platform-accountability regime comparable to the Digital Services Act.¹³
- The Digital Personal Data Protection Rules, 2025 ¹⁴operationalise the Act through consent-manager and data-fiduciary obligations; however,

¹⁰ Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

¹¹ Regulation (EU) 2024/1689, *supra* note 3.

¹² Digital Personal Data Protection Act 2023 (Act 22 of 2023) (India).

¹³ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L 277/1.

¹⁴ Digital Personal Data Protection Rules 2025 (India).

their application to biometric and behavioural data collected by immersive platforms remains unclear.

- The proposed Digital India Act¹⁵, intended to replace the IT Act, 2000¹⁶, seeks to address platform accountability and AI-generated content. However, as it remains under consultation, it is uncertain whether it will adequately address metaverse-specific legal challenges.

3. What India must Avoid

- India should not ignore the platform accountability
- The users must get protection against the wrongful content, don't wait for harm to occur, and against manipulation.

B. South Korea

South Korea has taken a proactive role in Metaverse regulation and tried to support. in South Korea, rather than relying solely on existing metaverse-related matters in existing legislation, where appropriate, legislation and regulatory structures are created specifically with the challenges of metaverse immersive virtual environments.

1. Key Legal Provisions & Approaches

- South Korea has taken a proactive stance by introducing metaverse ethics principles that help in the regulation of avatar behavior or actions, virtual harm, and platform conduct
- **Focus Areas:** Open Metaverse platforms, XR, 5G, and AI infrastructure, and Human capital development

2. India: Comparative Status & Gap

- India lacks the behavioral code or the enforceable ethics for

¹⁵ Digital Personal Data Protection Act 2023 (Act 22 of 2023) (India).

¹⁶ Information Technology Act 2000 (Act 21 of 2000) (India).

immersive environments or spaces.

- Do not regard virtual harm as "not real"
- Exposing users to emotional and psychological security

3. What India must Avoid

- Don't treat virtual harm as "not real"
- Avoid ignoring behavioral harms: emotional and psychological safety matters

C. United States

1. Key Legal Provisions & Approaches

- Courts are shaping the provisions through NFTs,
- The smart contract cases are determined on securities classification
- FTC cracks down on deceptive practices like false advertising by:
 - Children's Online Privacy Protection Act (COPPA)¹⁷
 - California Consumer Privacy Act (CCPA)¹⁸
 - Computer Fraud and Abuse Act (CFAA)¹⁹

2. India: Comparative Status & Gap

- India's judiciary is catching up with the digital disputes, yet lacks certainty on its stance on NFTs regulation, and enforcing smart contracts hinders.

3. What India must Avoid

- Don't wait for case law alone and take action
- Proactive regulation is better than reactive litigation

D. Japan

Japan has demonstrated a proactive approach to regulating and developing the

¹⁷ Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (USA).

¹⁸ California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq. (USA).

¹⁹ Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (USA).

Metaverse and Web 3.0 industries by establishing a Web 3.0 Policy Office within the Ministry of Economy, Trade, and Industry (METI).

1. Key Legal Provisions & Approaches

- Japan's intellectual property promotion plan 2022²⁰ covers metaverse
- Specialized Licensing and ownership of content have rules for virtual content and IP ownership in the Metaverse

2. India: Comparative Status & Gap

- India recognizes digital assets but lacks a licensing and content protection framework to clearly establish virtual property rights or standards for liability for immersive medium platforms

3. What India must Avoid

- Do not leave creators vulnerable
- digital intellectual property requires tangible legal protection.
- Building of interdisciplinary task forces for law, tech, psychology, ethics, and to shape holistic policy

Metaverse is about enhancing protection under the law of personal and biometric data gathered in virtual environments is important for user dignity in digital spaces. This supports rules that protect personal data in the Metaverse and uphold our dignity and privacy in these online areas.

E. Pakistan

1. Key Legal Provisions & Approaches

- Pakistan has no such extraordinary legislation concerning the Metaverse. Instead, its cybercrime law (Pakistan Electronic Crimes Act 2016)²¹ provides a general framework for addressing cybercrime and

²⁰ Japan Cabinet Office, Intellectual Property Promotion Plan 2022.

²¹ Pakistan Electronic Crimes Act (PECA), No. XL of 2016.

digital harm but does not specifically regulate immersive environments or virtual identities.

- Pakistan's PECA enforcement mechanisms may, in certain contexts, be more robust than comparable enforcement practices in India.

2. India: Comparative Status & Differences

- India's Information Technology Act, 2000 provides a more developed legal framework, although enforcement challenges remain in immersive digital environments.

3. What India Must Avoid

- Reliance solely on general digital laws may be insufficient to address metaverse-specific harms.
- Effective governance of the metaverse requires tailored regulatory and enforcement mechanisms.

India has made significant progress in digital innovation; however, it continues to face challenges in developing a comprehensive regulatory framework for metaverse governance.

V. CASE LAWS

1. Hermes v. Rothschild (USA, 2023)

- **The Issue:** Can someone create and sell digital replicas of Hermès' famous Birkin bags, calling them "MetaBirkins"?²² Artist Mason Rothschild minted NFTs depicting furry bags styled after the classic Birkin. Hermès stepped in, claiming trademark infringement.
- **The Judgment:** The court ruled in favor of Hermès, affirming that NFTs don't escape trademark laws.

This case serves as a crucial reminder; virtual items still need to respect real-world branding. If you're creating virtual fashion or environments, don't assume you can just remix well-known designs without consequences.

²² Hermès Int'l v. Rothschild, No. 22-CV-384 (S.D.N.Y. 2023).

2. Friel v. Dapper Labs (USA, 2023)

- **The Issue:** Are NFTs merely collectables, or do they qualify as financial securities? Dapper Labs sold NBA Top Shot NFTs, leading buyers to argue that these NFTs should have been registered as securities.²³
- **Judgment:** The court refused to dismiss the case at an early stage, indicating that certain NFTs could potentially satisfy the requirements of the Howey Test and be treated as securities. This decision highlighted the possibility of increased financial regulation within metaverse and NFT ecosystems.
- **Subsequent Development:** However, the litigation was settled in June 2024 through a US\$4 million agreement. The plaintiffs agreed to cease asserting that NBA Top Shot NFTs were securities, while Dapper Labs maintained that the NFTs were digital collectibles rather than securities. Consequently, the case did not result in a final judicial determination on the securities question

3. CNIL vs. Worldcoin (France, 2023)²⁴

- **The Issue:** Is it ethical to use iris scans to provide users with a digital ID?
- **What Happened:** Worldcoin initiated iris scans to verify identities for crypto distribution, prompting an investigation by France's data protection authority.
- **The Judgment:** CNIL raised serious privacy concerns, and the case remains ongoing.

This case highlights the intense scrutiny around privacy in immersive platforms. If your Metaverse collects biometric data or emotional feedback, be prepared to prioritize consent and ethical practices.

4. Italy vs. Replika AI (2023)

- **The Issue:** Can AI chatbots safely interact with minors in immersive

²³ Friel v. Dapper Labs, Inc., No. 1:21-cv-05837-VM (S.D.N.Y.).

²⁴ CNIL, Investigation Report on Worldcoin's Biometric Data Practices, France (2023).

environments?²⁵

- **What Happened:** The Garante per la protezione dei dati personali found that Replika's processing of Italian users' personal data raised serious GDPR concerns, particularly in relation to minors and emotionally vulnerable persons. Acting through an urgent order dated 2 February 2023, the Garante temporarily restricted Luka Inc. from processing the personal data of users located in Italy until adequate compliance measures were adopted.
- **The Judgment:** Replika was denied access in Italy.

This case underlines the importance of child protection—both online and in virtual spaces. If your Metaverse features chat options, consider implementing age restrictions and content moderation.

5. South Korea's Metaverse Ethics Guidelines (2022-ongoing)

- **The Issue:** How do we manage avatar conduct and prevent virtual harm?²⁶
- **What Happened:** Instead of waiting for lawsuits, South Korea proactively issued ethical guidelines for behavior in immersive platforms.
- **The Judgment:** This isn't a court ruling, but a forward-thinking policy initiative.

South Korea is pioneering behavioral regulations. They're addressing critical questions like avatar harassment and real-world impacts of virtual actions. These guidelines could shape future legislation.

6. Japan's IP Promotion Plan & Metaverse Reports (2022-2023)

- **The Issue:** Who truly owns digital content in the Metaverse, and who is liable when issues arise?²⁷
- **What Happened:** Japan released legal studies to tackle challenges

²⁵ Garante per la protezione dei dati personali, Provvedimento n. 39 del 2 febbraio 2023, Replika/Luka Inc. (Italy).

²⁶ South Korea Ministry of Science and ICT, Metaverse Ethics Guidelines (2022-ongoing).

²⁷ Japan Cabinet Office, Intellectual Property Promotion Plan 2022 (2022).

posed by the Metaverse.

- **The Judgment:** While not judicial, this work lays an essential foundation for future regulations.

Japan is laying the groundwork for legal frameworks in immersive environments, tackling licensing, platform responsibility, and user safety before potential legal disputes arise.

7. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), Supreme Court of India

- **Issue:** Is privacy a fundamental right protected by the Indian Constitution?²⁸
- **Judgment:** In a landmark decision, a 9-judge bench unanimously ruled that privacy is indeed a fundamental right under Article 21.

This case is a cornerstone for digital rights in India. It sets the stage for challenging intrusive technologies like biometric surveillance and AI profiling along with Metaverse platforms that gather behavioral data. Essentially, it means that any immersive technology must respect user autonomy and consent.

8. Banyan Tree Holding Pvt. Ltd. v. Murli Krishna Reddy (2008), Delhi High Court

- **Issue:** Can Indian courts have power over a foreign website that targets Indian consumers?²⁹
- **Judgment:** The court ruled that being simply present in India will not suffice; there should be a clearly defined interaction or business intention.

It's significant in terms of understanding who has authority under law in the Metaverse. If a non-Indian platform engages with Indians in another country, say, selling or if there is interaction, then Indian courts might be involved. It helps explain

²⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) (establishing privacy as a fundamental right under Article 21 of the Constitution).

²⁹ Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy, 2010 (42) PTC 361 (Del.) (Division Bench, decided 23 November 2009).

the difference between just being online and really going after a market.

9. Digital Collectibles Pte Ltd v. Galactus Funware Technology Pvt. Ltd., Delhi High Court (2023)

- **Issue:** Whether the use of cricketers' names, images, and player attributes in NFT-enabled fantasy sports player cards infringed personality and publicity rights.
- **Judgment:** The Delhi High Court refused to grant interim injunction in favour of Digital Collectibles/Rario. Justice Amit Bansal held that the right of publicity is not absolute in India and must be balanced against the right to freedom of speech and expression under Article 19(1)(a) of the Constitution. At the interim stage, the Court found that MPL/Striker's use of player names, images, and publicly available match information in its NFT-enabled fantasy sports game did not amount to infringement of personality rights. The Court further observed that Rario could not claim exclusivity over NFT technology itself, as such technology is freely available.
- **Importance:** This decision is significant because it qualifies, rather than expands, personality-rights protection in the NFT context. It indicates that the use of publicly available player information in NFT-enabled fantasy platforms may be protected where it is connected to speech, information, or fantasy-sports activity and does not falsely suggest endorsement or exclusive association. The case therefore demonstrates that Indian courts may balance publicity rights against constitutional free-expression interests when assessing NFT-based digital assets. It does not establish that personality rights automatically extend to all NFT-based virtual property.

10. Zanmai Labs Pvt. Ltd. v. Bitcipher Labs LLP, Bombay High Court (2025)

- **Issue:** What duties does a crypto exchange owe to consumers with respect to virtual digital assets held on their account?³⁰

³⁰ Zanmai Labs Pvt. Ltd. v. Bitcipher Labs LLP (Bom. H.C. 2025).

- **Judgment:** The Bombay High Court ruled that a crypto exchange is a virtual digital asset trustee and holds a fiduciary relationship with its users.
- **Impact:** This is the certified, public 2025 Bombay High Court decision on custody of crypto-assets.

VI. UNRESOLVED QUESTIONS: VIRTUAL PROPERTY AND CONSUMER PROTECTION IN INDIAN COURTS

Neither an Indian court has decided if the virtual land available on a metaverse platform can be acquired by way of adverse possession nor is it established as to whether the same may be considered property of sorts as per the Indian law. The same is an open legal issue that perhaps can be contemplated as metaverse-based transactions develop.

In the same vein, whether the inclusion of such open-ended refund policies or such unilateral changes in the contracts may be considered as an 'unfair trade practice' is also unestablished under sec.2(47) of the Consumer Protection Act, 2019.³¹ While such an argument is legally plausible, it has not yet been authoritatively tested before Indian consumer forums or courts.

VII. SUGGESTIONS AND RECOMMENDATIONS

1. Reactive regulation: taking action only after harm has been done. Preventive measures and anticipation are necessary.
2. Over-Centralization: End users' freedom and creativity may be impeded by government control over the Metaverse.
3. Ignoring Behavioral Damage: It is important to consider psychological and emotional safety in digital settings as tangible and legally significant.
4. Vague Enforcement: Legislation must be upheld by competent regulatory bodies, not by wishful thinking.

³¹ *Consumer Protection Act 2019* (Act 35 of 2019) s 2(47) (India).

5. Create a new Metaverse Code of Conduct or update existing ones. State rights and duties for individuals, websites, and personas including security, name, and behavior.
6. Explain Contracts and Virtual Property. Provide legal definitions for smart contracts, digital assets, and networks, and enable dispute resolution.
7. Construct a Sandbox for Regulations. To promote innovation without sacrificing security, let tech companies and startups test immersive technologies under close legal supervision.
8. Established a multidisciplinary task force, get a team of knowledgeable attorneys, technologists, psychologists, and policy experts to create a comprehensive and dynamic metaverse regulatory framework.
9. Participate in Global Treaty Discussions
10. India should try, either become a participant or lead international standards for governance regulation on the Metaverse, ensuring cross-national protection and responsibility of its citizens
11. India has the human capital, infrastructure, and juridical tradition to be a leader in this field, but it must act with conviction, compassion, and vision.

VIII. CONCLUSION

Indian law currently has a number of tools available to combat online crime. The Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Copyright Act, 1957, and the Trade Marks Act, 1999 collectively address fraud, harassment, and the protection of intellectual property across chat applications, social media, websites, and other familiar digital platforms

The difficulty, as this paper has shown, is that laws designed for the conventional internet do not readily extend to the far more complex environment of the metaverse. The comparative analysis in Part VIII demonstrates that the European Union, South Korea, the United States, and Japan have each begun to develop tools — whether through data protection law, behavioural codes, securities regulation, or IP-licensing frameworks — that India has yet to adopt in comparable form, while the case-law survey in Part IX shows that several of the harms this paper identifies (avatar

harassment, virtual property disputes, and unfair EULA terms) remain genuinely untested before Indian courts.

This is not to say that existing Indian law offers no protection: a person whose work is stolen, or who is defrauded online, retains a route to legal recourse. But the metaverse gives rise to new categories of harm and dispute that do not map neatly onto these traditional protections, and the Research Gap identified in Part VII – spanning the absence of a metaverse-specific law, weak platform accountability, the absence of behavioural codes, limited judicial engagement, the lack of international alignment, and the unresolved reach of the newly enacted Bharatiya Nyaya Sanhita, confirms that India's current framework, though a reasonable starting point, is not adequate to the task.

Taken together with the recommendations set out in Part X, the analysis in this paper points to a single conclusion: incremental interpretation of existing statutes is unlikely to suffice. What is required is a combination of targeted amendment to the Information Technology Act, the enactment (rather than continued deferral) of a Digital India Act genuinely responsive to metaverse-specific harms, and the institutional reforms, a behavioural code, a regulatory sandbox, and a multidisciplinary task force recommended above. Proactive legal innovation of this kind is essential if India is to navigate the evolving digital frontier and transform the metaverse into a secure, rights-protective space for its citizens.

IX. REFERENCES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
2. Digital Personal Data Protection Act, No. 22 of 2023, India Code.
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).
4. Information Technology Act, No. 21 of 2000, India Code.
5. R R Krishnaa, 'Challenges in the Metaverse Jurisdiction and International Treaty Law' IRPJ (2023) <https://irpj.euclid.int/articles/challenges-in-the-metaverse-jurisdiction-and-international-treaty-law/>

6. 'Identity, Crimes, and Law Enforcement in the Metaverse' Humanities and Social Sciences Communications (2023)
<https://share.google/4xZW24FQYUE53y3XL>
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
8. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (Digital Services Act), 2022 O.J. (L 277) 1.
9. California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq. (USA).
10. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (USA).
11. Japan Cabinet Office, 'Intellectual Property Promotion Plan 2022'
<https://www.japan.go.jp/ip/metaverse>
12. Pakistan Electronic Crimes Act (PECA), No. XL of 2016.
13. Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code.
14. Digital Personal Data Protection Rules, 2025, India Code.
15. Ministry of Electronics and Information Technology, Government of India, Draft Digital India Act, Consultation Paper (2023).
16. Hermès Int'l v. Rothschild, No. 22-CV-384 (S.D.N.Y. 2023).
17. Friel v. Dapper Labs, Inc., No. 1:21-cv-05837-VM (S.D.N.Y.).
18. Commission Nationale de l'Informatique et des Libertés (CNIL), Investigation Report on Worldcoin's Biometric Data Practices, France (2023).
19. Garante per la protezione dei dati personali, Provvedimento n. 39 del 2 febbraio 2023, Replika/Luka Inc. (Italy).
20. Jean Baudrillard, *Simulacra and Simulation* (Sheila Faria Glaser trans., Univ. of Mich. Press 1994) (1981).
21. *Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy*, 2010 (42) PTC 361 (Del. HC.).
22. *Digital Collectibles Pte Ltd v. Galactus Funware Technology Pvt. Ltd.*, CS(COMM) 108/2023 (Del. H.C. 2023).
23. *Zanmai Labs Pvt. Ltd. v. Bitcipher Labs LLP*, (Bom. H.C. 2025).
24. More Than Digital, 'History & Evolution of the Metaverse Concept'

<https://morethandigital.info/en/history-evolution-of-metaverse-concept/>

accessed 26 August 2026.

25. Wikipedia, Virtual Reality, https://en.wikipedia.org/wiki/Virtual_reality (last visited Aug. 26, 2026).
26. Wikipedia, Augmented Reality, https://en.wikipedia.org/wiki/Augmented_reality (last visited Aug. 26, 2026).
27. Wikipedia, Hyperreality, <https://en.wikipedia.org/wiki/Hyperreality> (last visited Aug. 26, 2026).