INTERNET POLICY REVIEW

Volume 15 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Navigating legal complexities of metaverse interoperability: A comparative study of governance models of EU and India

Aswathy Prakash G. *Saveetha School of Law*
Yochana Rajan *Jindal Global Law School*

DOI: https://doi.org/10.14763/2026.3.2110

Published: 24 September 2026
Received: 17 November 2025 **Accepted:** 12 May 2026

Funding: The authors did not receive any funding for this research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Prakash G., A., & Rajan, Y. (2026). Navigating legal complexities of metaverse interoperability: A comparative study of governance models of EU and India. *Internet Policy Review*, *15*(3). https://doi.org/10.14763/2026.3.2110

Keywords: Cross-platform functionality, Inclusivity, Sustainability, Collaboration, Innovation

Abstract: With the metaverse unfolding as a living digital environment, its interoperability between platforms presents intricate legal and regulatory issues. This research performs a comparative analysis of governance paradigms within the European Union (EU) and India in the context of their regulatory responses to metaverse interoperability, portability of data, and preservation of digital rights. By analysing the regulatory environments of both jurisdictions, the study recognises key challenges and explores policy options for achieving a smooth and secure virtual space. In the context of the EU, established frameworks like the General Data Protection Regulation (GDPR), Digital Services Act (DSA), Digital Markets Act (DMA), and the newly enacted Artificial Intelligence Act (AI Act) define the governance approach for digital platforms, including those within the metaverse. India, on the other hand, appears to have the technical and demographic foundations for the metaverse, but is in the nascent stage of metaverse technology regulation. Through the comparison of the EU's rule-based regulatory approach with India's dynamic digital policy environment, this research adds to the general metaverse governance debate. It argues that the structural divide between these two frameworks creates a regulatory vacuum, leaving users unprotected when moving across different platforms. To resolve this issue, the paper introduces a hybrid policy model. This approach integrates the EU's proactive compliance standards with India's unique infrastructure and sovereignty constraints.

This paper is part of **Governing the metaverse through the lens of the public sphere**, a special issue of *Internet Policy Review* guest-edited by Annelieke A.M. Mooij and Sunimal Mendis.

Introduction

The rise of the metaverse, surrounding immersive digital environments, digital avatars, tokenised assets, such as Non-Fungible Token (NFTs), and cross-platform social experiences, brings the issue of interoperability to the forefront of technology law and policy. Interoperability in the context of metaverse refers to its ability to interact, exchange, and make use of data to enable its movement, transactions, and participation across diverse platforms and jurisdictions. It not only refers to the technical ability for users to transfer avatars, assets, and personal data seamlessly across different platforms but also to the crucial legal foundations that govern such exchanges. (Yang et al., 2024) These include questions of identity continuity, asset ownership, privacy, and user control over personal and behavioural data, all of which are realised within a patchwork of national and supranational legal regimes. Concrete metaverse use cases such as avatar portability (the transfer of digital personae and authentication attributes from one platform to another), asset migration (including NFTs and virtual goods), and robust data portability rights (the ability for users to export and carry their data across services) exemplify the high stakes and complexity of this interoperability challenge (Rawat et al., 2024). While recent technical proposals, such as the application of Self-Sovereign Identity (SSI) protocols and off-chain governance agreements, have shown promise, they only partially address interoperability issues (Grüner et al., 2021). Their effectiveness remains contingent upon the harmonisation of underlying legal requirements (Laborde et al., 2023). These include norms related to privacy, data protection, and cross-border data flows (Sorrentino & López-Guzmán, 2025a, 2025b).

Defining the metaverse: A working framework

Ever since Neal Stephenson introduced the term '*the metaverse*' in his 1992 novel *Snow Crash*, it has outgrown its origin to accumulate competing definitions. It now spans into vast technological territories from Virtual Reality (VR) networks to blockchain markets, making it difficult to pin down into a uniform legal definition (Dwivedi et al., 2022). For this paper, we adopt the European Commission's operational definition, which describes virtual worlds as 'persistent, immersive environments based on technologies such as 3D and extended reality (XR) which make it possible to blur the lines between physical and digital worlds in real time for the

purposes of working, socialising, learning, providing entertainment, designing and carrying out financial transactions' (European Commission, 2023). This definition is preferred for three reasons: it is jurisdiction-specific to the EU framework under analysis; it remains technology-neutral, encompassing both current VR/AR platforms and emerging brain-computer interface environments. Further, it operates as a function-oriented approach, focusing on user activities rather than a platform specific technical architecture. It is, however, important to note that the European Commission deliberately avoids the term 'metaverse' in its 2023 Web 4.0 and Virtual Worlds Strategy, a choice that is inherently regulatory in character, signalling the EU's preference for a human rights-grounded vocabulary over the Silicon Valley-inflected branding (Martini, 2025). India has not adopted an equivalent official definition. For consistency, this paper uses 'metaverse' to denote persistent, immersive, avatar-mediated, and multi-platform digital environments where interoperability challenges typically arise. We apply this definition to global platforms like Meta Horizon Worlds, Roblox, Decentraland, and The Sandbox, alongside Indian-developed counterparts such as Tech Mahindra's TechMVerse and Reliance Jio's emerging immersive ecosystem.

This study argues that the structural divide between the EU’s rights-focused laws and India's sovereignty-driven framework creates a major regulatory vacuum. As a result, virtual world users experience the risks of cross-platform participation without the necessary legal protections to ensure their safety. The EU's proactive, rights-based system offers a structurally stronger foundation than India's model. To be fair, India's Digital Personal Data Protection (DPDP) Act does introduce ex-ante obligations for corporate data fiduciaries. However, the broader Indian system remains highly reactive and centered on basic consent architectures. The EU framework remains blind to virtual assets and avatar sovereignty, while India’s statutory framework fails to translate its constitutional privacy baselines into active cross-platform obligations. To bridge this divide, this study rejects simple regulatory copy-pasting, arguing instead for a localised hybrid regulatory architecture that integrates the EU’s rights-constitutive design principles with India’s unique digital sovereignty and infrastructural scale. This doctrinal inquiry is methodically organised around the technical, rights-based, and institutional layers of interoperability.

To contextualise this study, we must examine the academic debate regarding what interoperability truly means and whose interests it supports. Many researchers challenge the assumption that system compatibility is inherently good. Specifically, Archer, Ravn, and Thylstrup (2025) argue that common views on the topic rest

on two flawed beliefs. The first is that isolated data systems are completely dysfunctional. The second is that breaking down these boundaries always helps users rather than the tech companies themselves. These authors argue that forcing systems to open up can backfire. Instead of reducing the power of dominant tech firms, it can actually help them consolidate their market control. In a similar vein, Huber (2025) examines US healthcare data rules to show that mandatory data sharing can become a tool for private profit extraction. Trauttmansdorff (2022) provides a parallel critique in the border governance context, arguing that treating system compatibility as a neutral technical solution serves a deliberate political purpose. Specifically, it hides the deeper power dynamics and governance choices built into technical standards. In the metaverse, the risk of private market control through open systems is highly present. This is especially true when dominant companies like Meta control both the primary virtual worlds and the underlying software interfaces. This paper maintains a deliberate, focused scope. Rather than debating the economic politics of system compatibility, this study answers a more immediate question. Given that the EU and India already promote platform openness and data portability, what legal flaws stop these frameworks from protecting users in virtual environments? We do not assume that interoperability is automatically perfect. Instead, we evaluate whether existing rules can successfully put user rights ahead of platform control. Therefore, the paper takes a rights-focused approach to ask how law can make data sharing safer and more accountable, while leaving wider economic debates outside its legal scope.

The EU and India as metaverse governance test cases: Market context

The EU-India comparison is not merely a doctrinal exercise: it reflects two of the most consequential emerging metaverse markets. According to analysis from Market Research Future, the European metaverse market was valued at approximately USD 4.66 billion in 2024. This market is projected to expand significantly from USD 6.17 billion in 2025 to USD 100.90 billion by 2035, exhibiting a robust compound annual growth rate (CAGR) of 32.25% (Dhapte, 2026). While this trajectory is heavily driven by global infrastructure players like Meta, Microsoft, and NVIDIA, the regional landscape is further shaped by localised, state-led initiatives like the EU's CitiVerse smart city program. Driven by this state-backed momentum, European governments, including France and Germany, committed an estimated EUR 3.4 billion in public R&D amid a user base that expanded by 28% in 2025 (OECD, 2026).

However, the market space remains dominated by the aforementioned US-head-

quartered tech giants. Although foreign-built, these platforms are pulled into the EU regulatory orbit via the GDPR's extraterritorial reach and the DMA's gatekeeper obligations. (Jena, 2018) This configuration creates the precise structural friction under analysis: architectures designed under American legal assumptions are forced to adjust to Europe's rights-based interoperability mandates.

India presents a structurally different but equally significant picture. The Indian metaverse market was valued at approximately USD 6.60 billion in 2024 and is projected to reach USD 231.82 billion by 2035 (Munde, 2025). Critically, India is not merely a consumer market for foreign platforms; it functions as an active production ecosystem. Domestic technology leaders like Reliance Jio, Tech Mahindra, TCS, Infosys, and HCL Technologies are rapidly deploying localised architectures such as JioGlass, TechMVerse, Avapresence, Metaverse Foundry, and Metafinity. However, this domestic infrastructure operates in a relative regulatory vacuum: while India's DPDP Act 2023 governs basic data processing, it remains silent on spatial data portability, avatar sovereignty, and structural interoperability standards. The scale of this regulatory gap is underscored by India's internet subscriber base, which stood as the world's second-largest at approximately 969 million in early 2025 (Telecom Regulatory Authority of India, 2025). The migration of even a nominal percentage of these users into avatar-mediated spaces effectively transforms the legal anomalies identified throughout this study into pressing, real-time enforcement and governance challenges.

A comparative evaluation of the EU and Indian frameworks is uniquely instructive, yet it requires an explicit engagement with their inherent structural and institutional divergence. While the EU relies on a deeply codified, rights-based regulatory framework with an established tradition of market enforcement, India's approach is driven by a digital-first, infrastructure-led model designed to accelerate domestic innovation. Despite these institutional differences, pairing these two jurisdictions is highly valuable. They represent two of the most consequential, non-aligned regulatory testing grounds outside of the United States and China. By evaluating how a prescriptive, rights-centered architecture (the EU) and an infrastructure-driven, emerging digital market (India) independently grapple with the legal mechanics of virtual spaces, this study uncovers the foundational global friction points of metaverse interoperability.

Despite the clear commercial weight of these markets, the existing literature reveals significant limitations. Notably there is a clear dearth of thorough, metaverse-specific statutory analysis juxtaposing the legal mandates of the EU and India with one another (Guhathakurta, 2024). While many of the current studies offer

extensive comparisons of privacy and data protection policies, and others review cross-border data flow clauses (IBA Intellectual Property, Communications and Technology Law Committee, 2024; Nath, 2025), very few methodically map how these legal frameworks handle, or fail to handle, the particular challenges raised by avatars, NFT, and asset portability, and the adjudication of digital rights in interoperable metaverse scenarios (M. Gupta, 2025; Duggal et al., 2023). Data portability and intellectual property rights represent two domains where this scholarly disparity is most evident (Pankhudi Khandelwal, 2024). In these spheres, statutory and doctrinal clarity is still lacking or is not adequately adapted to the reality of immersive, cross-platform ecosystems.

This study uses a comparative legal analysis to evaluate the regulatory landscape. Our primary sources include core laws like the GDPR, DSA, DMA, AI Act, IT Act, and the DPDP Act. We combine these with industry guidelines from the World Wide Web Consortium (W3C) and the Metaverse Standards Forum to examine how voluntary technical rules influence actual laws. We deliberately compare the EU and India instead of other options like the US or China. Both jurisdictions serve as highly influential, independent digital markets. While the EU relies on a rights-first model, India uses a state-centered approach, providing the sharpest available contrast to study how different legal philosophies handle virtual world compatibility. As a research caveat, this comparison involves a major imbalance in enforcement power. While EU data protection authorities possess decades of experience and full power to issue fines, India's Data Protection Board is still in its early stages. This difference limits a direct comparison of how effectively either system enforces its rules in the real world.

Section 1. Conceptualising interoperability in the metaverse

To evaluate these regulatory variations, we must first establish a clear framework for how data moves across virtual systems. Interoperability operates across three distinct layers. First, the technical layer deals with software protocols and data exchange standards. Second, the rights-based layer governs user protections like data portability, consent, and identity continuity. Third, the market-structure layer handles competition rules that force dominant platforms to open their infrastructure to rivals. At its architectural baseline, interoperability denotes the capacity of diverse, autonomous systems to securely exchange information and inherently utilise the data that has been exchanged. Before exploring its spatial application, it is vital to distinguish true technical interoperability from mere data portability.

While portability simply allows a user to download and transfer static data assets from one siloed ecosystem to another, true interoperability demands an active, real-time synchronisation of execution environments. In the context of the metaverse, this concept expands to denote the capability of users to experience a seamless, real-time exchange of their digital identities, virtual assets, data tokens, and governance protocols across varied, competing virtual platforms (Rawat et al., 2024). This structural continuity enables users to maintain consistent and uninterrupted interactions across different metaverse environments.

This multi-layered concept, though technologically driven, rests fundamentally on a dual-action legal architecture: legal frameworks must enable the technical baseline of interoperability while mandating its structural enforcement. On the one hand, the law acts as an enabler by establishing harmonised public standards, intellectual property cross-licensing systems, and safe harbours that allow competitive systems to communicate safely. On the other hand, the law operates as a strict mandate, as exemplified by the EU's Digital Markets Act, by legally forcing dominant digital gatekeepers to open their proprietary interfaces to third-party developers.

To bridge this legal necessity with practical software execution, developers rely on specific architectural innovations that translate statutory mandates into functional code. Foremost among these structural innovations supporting metaverse interoperability is Self-Sovereign Identity (SSI). This system decentralises identity management by allowing users to retain sovereign control over their personal data and digital credentials, which include avatar attributes and associated metadata (Weigl et al., 2023). For instance, Laborde et al. (2023) propose an SSI-based interoperability scheme ensuring that avatars retain compatibility and data continuity as users migrate between platforms. This mechanism directly operationalises compliance-by-design requirements by safeguarding user autonomy while providing a practical direction toward privacy-preserving technical interoperability.

On the asset layer, another vital technical mechanism involves open APIs and standardised digital asset protocols. Protocols like OpenXR and NFTs facilitate cross-platform portability and consistent rendering of 3D assets across competitive ecosystems (Hatami et al., 2024; Gowda, 2025). Currently, these technical baselines are being codified by collaborative industry groups such as the Metaverse Standards Forum and the W3C (Chen et al., 2023). The W3C focuses specifically on establishing rigid technical specifications like decentralised identifiers (DIDs) and verifiable credentials (VCs), which are rapidly becoming central to the structural and compliance infrastructure of the modern metaverse (Mazzocca et al., 2025).

Legal and technical design of interoperability: EU and India

Legal frameworks directly influence how technical interoperability plays out in practice. For instance, data portability, and privacy rights, as defined by the EU GDPR and India's DPDP Act, establish the rules governing how user data can be transferred, accessed, or deleted (Panchal, 2024). Crucially, the relationship between emerging technological architectures like SSI and these legal norms are fundamentally complementary yet friction-ridden. While SSI protocols natively codify compliance-by-design mechanisms by handing decentralised data control back to the user, a severe operational gap emerges when statutory frameworks define data portability in narrow, static terms. This regulatory friction limits the dynamic, real-time synchronisation required when personal attributes span multiple competing virtual jurisdictions (Afzal, 2024). Intellectual property law introduces another under-examined dimension, especially the ownership and cross platform governance of virtual assets. Determining the enforceability of rights over user-generated content, royalty structures, and licensing terms remains highly ambiguous when digital assets migrate between platforms (Kowalski & Nowak, 2023). This institutional gap highlights the lack of precise legal guidance on asset provenance, cross-platform recognition, and mutual enforcement mechanisms (Giacalone & Arnone, 2024).

To evaluate these software-embedded solutions, this study intentionally adopts the framework of compliance-by-design rather than the narrower concept of privacy-by-design. While privacy-by-design traditionally focuses on data protection principles such as minimisation and confidentiality, compliance-by-design operates as a broader regulatory paradigm. It demands the structural embedding of all multi-layered statutory rules, spanning data privacy, technical interoperability mandates, and digital asset governance directly into the original platform architecture.

To methodically analyse these inadequacies across the EU and Indian landscapes, **Table 1** evaluates nine core regulatory parameters. These parameters are deliberately selected to the exclusion of broader legal domains because they map systematically onto the three operational layers of metaverse interoperability: the institutional layer, the identity layer, and the cross-border data layer. Firstly, regulatory authority and status of regulation establish the institutional maturity and enforcement body required to resolve multi-platform conflicts. Secondly, the identity and asset layers are evaluated through data portability rights, avatar applicability, consent requirements, and explicit statutory focus on interoperability, which collectively govern the legal status and transfer mechanics of the virtual persona. Finally, cross-border data transfer, metaverse-specific clarity, and the technical-legal

interface determine how localised architectures can legally and technically move interactive data assets across sovereign infrastructure boundaries. Together, these nine dimensions form a comprehensive background designed to isolate where technical continuity collides with statutory friction.

TABLE 1: Current Interoperability Regulatory framework under GDPR and DPDP Act (Source: Researcher's own compilation based on secondary data)

CATEGORY	EUROPEAN UNION (GDPR) [EU]	INDIA (DPDP ACT) [IN]
Regulatory authority	Data Protection Authorities (DPAs) of Member States.	Data Protection Board of India (DPBI).
Data portability rights	Explicitly provided under Article 20 of GDPR; includes the right to receive and transfer personal data.	No explicit data portability right; transfer depends on notice and consent frameworks.
Applicability to avatars / Virtual identities	Indirectly applicable; avatars treated as personal data if linked to identifiable individuals.	Avatars/data considered personal if identifiable; coverage likely through broad personal data scope.
Consent requirements	Strict consent regime; must be informed, specific, and revocable.	Emphasises "notice and consent" model; deemed consent permitted in certain circumstances.
Cross-border data transfer	Allowed with adequate safeguards (Standard Contractual Clauses, Adequacy Decisions, etc.).	Restricted to countries notified by the government; conditions apply but not elaborated in detail.
Focus on interoperability	Data portability and machine-readable formats intended to support	No metaverse- or interoperability-specific

CATEGORY	EUROPEAN UNION (GDPR) [EU]	INDIA (DPDP ACT) [IN]
	interoperability.	provisions; general data fiduciary duties apply.
Clarity on metaverse-specific scenarios	Lacks specific metaverse guidance; principles can be interpreted to apply.	No mention of metaverse or immersive environments in statute.
Technical-legal interface	Mandates data protection by design (Article 25), establishing the statutory baseline for a broader compliance-by-design framework.	No built-in alignment with technical design; scope for future integration of compliance-by-design.
Status of regulation	In force since 2018.	Enacted in 2023; rules notified in Nov. 2025, but institutional setup still under development.

The regulatory divergence and statutory omissions highlighted in Table 1 demonstrate that while legal frameworks are maturing, several architectural challenges persist when applying traditional privacy rules to interoperable virtual worlds. One continuing challenge is the handling of mixed datasets that contain both personal and non-personal information, such as behavior-based profiles formed through user activity (Strecker et al., 2025) Avatars and immersive experiences produce sensitive data, such as facial expressions, voice patterns, and behavioral indications. Such data types are not fully captured under current privacy laws, leaving users without sufficient clarity regarding their rights and platforms without defined obligations (Eltanbouly et al., 2025; Renieris, 2023). Few studies emphasise the regulatory shortcomings surrounding consent mechanisms and user control in these contexts and argue for urgent legal reforms alongside technical safeguards like transparency and user-access controls (Sorrentino & López-Guzmán, 2025a, 2025b).

To resolve this bottleneck, current scholarship heavily emphasises "compliance-by-design" frameworks, which advocate for embedding core legal protections, such as user consent and active interoperability architectures, directly into the software foundations of metaverse platforms (Laborde et al., 2023; Casanovas et al., 2022). Laborde et al. (2023) demonstrate the viability of this approach by aligning technical interoperability protocols with legal obligations derived from instruments like the GDPR. Their model integrates policy expectations into the functioning of metaverse architectures. Nonetheless, this approach cannot succeed in isolation, as technical fixes alone cannot ensure user protection unless backed by enforceable legal rights. The literature consistently urges closer alignment between tech-

nical standard-setting and legal requirements (Brownsword, 2024). Organisations like the Metaverse Standards Forum and W3C are developing foundational tools, yet these efforts often outpace the legal grounding required to ensure enforceability and accountability (Garon, 2022). In the metaverse the power of setting technical standards is not only in the hands of the government but also of big tech companies and civil society (Martini, 2025). The EU, for example, aims to assert its regulatory principles globally through involvement in these technical forums. Yet this geopolitical ambition is undermined by the absence of detailed legal mappings that connect technical protocols to statutory rights or binding transnational agreements.

Moreover, the legal status of the standards produced by the Metaverse Standards Forum and the W3C remains strictly non-binding, operating as voluntary consensus frameworks or soft law. These specifications lack independent statutory enforceability, gaining regulatory authority only when sovereign states absorb them into hard legislative texts. Within the EU context, this integration is managed directly via the European Commission's rolling plan for ICT standardisation. Rather than duplicating technical rules, the EU utilises these standardisation requests to build a legal 'presumption of conformity' under binding market laws that forces designated gatekeepers to maintain well-suited open architectures.

India's engagement with these standard-setting associations, on the other hand, follows a structurally distinct, market-led path rather than a direct state mandate. While the Bureau of Indian Standards monitors global developments, the primary route for Indian integration into the W3C and Metaverse Standards Forum is driven by the state's dominant domestic technology companies such as Tata Consultancy Services, Infosys, Tech Mahindra, and Reliance Industries, who maintain active institutional memberships to anchor their localised platforms within global models. However, this corporate engagement operates under a notable domestic statutory lag. India's DPDP Act 2023 establishes comprehensive data fiduciary obligations but completely lacks a regulatory bridge that recognises or mandates compliance with these international technical specifications. Consequently, while the EU actively weaponises soft law to engineer hard-law gatekeeper mandates, India relies on private industry adoption to maintain global compatibility. Hence, in Indian context, this strategic reliance leaves a critical enforcement void involving cross-platform metadata and identity portability within its domestic borders.

Section 2. The EU's regulatory framework and policy landscape

The European Union has established itself as a pioneer of ex-ante digital market regulation through a deeply integrated, rights-based protective approach (European Data Protection Supervisor, 2025). Rather than relying on fragmented post-hoc enforcement, this regulatory architecture blends general privacy protection with targeted rules for online marketplaces and digital services through the GDPR, the Digital Services Act (DSA), and the Digital Markets Act (DMA). For example, the DSA remodels platform liability by compelling Very Large Online Platforms (VLOPs) to mitigate systemic risks, explicitly targeting algorithmic harms, deceptive dark patterns, and dark-ad profiling (Turillazzi et al., 2023; Graef, 2019). Simultaneously, the DMA limits the power of dominant digital platforms. It forces these gatekeepers to provide open access to their software interfaces and bans them from favoring their own services over independent competitors (Hey, 2024; Geradin, 2021). This unified framework has a broad global reach that protects European users internationally. Any platform that processes the data or shapes the market options of EU residents must legally comply, regardless of its home country (Gstrain & Zwitter, 2021). This global reach illustrates what Bradford (2020) calls the "Brussels Effect." This concept describes the EU's unique ability to spread its legal standards worldwide through its market power rather than through formal international treaties.

As the EU begins to address increasingly immersive digital spaces like the metaverse, its comprehensive regulations provide an expansive foundation, but the system still struggles with severe gaps in tracking cross-platform data flows and executing laws across borders. Even so, digital identity representation is rapidly evolving. Although early studies highlighted a missing framework for virtual identities, the EU's new eIDAS 2.0 rules and the planned European Digital Identity (EUDI) Wallet establish a uniform, decentralised system to verify and protect user data across member states (Regulation (EU) 2024/1183, 2024). This infrastructure allows users to keep a continuous, verified identity across separate platforms. However, Article 20 of the GDPR presents deep regulatory challenges. Immersive environments require a constant, real-time exchange of user data between platforms. This fluid technical need directly opposes the GDPR's static mechanisms, which were designed for simple, one-time data downloads (Wolford, 2019).

Beyond privacy, the DSA establishes a vital framework for how user-generated content, virtual assets, and social interactions are managed within the metaverse. Although the DSA is primarily a content accountability law rather than an interoper-

ability instrument, its transparency and appeals obligations indirectly bear on metaverse governance. When platforms use algorithmic moderation to govern avatar conduct and virtual asset disputes, the DSA obligations make that governance logic legally contestable. Article 6 of the DMA directly addresses the infrastructure layer of these ecosystems by targeting technical gatekeepers (Mäihäniemi, 2025). It legally requires dominant platforms to provide competing services open access to the underlying software and hardware functionalities needed for interoperability (Article 6(7), DMA). For virtual worlds, this open access is essential to ensure the cross-platform compatibility of digital identities, avatars, and assets, directly preventing corporate vendor lock-in (Rombolà, 2023). However, detailed technical specifications and concrete enforcement mechanisms remain a work in progress under the DMA, particularly given the sensitive, real-time nature of immersive data flows.

This architecture is further reinforced by the EU AI Act, which applies a strict, risk-based classification system to immersive platforms. Depending on how they are designed, core metaverse elements like AI-driven avatars, virtual assistants, and real-time emotion detection algorithms are highly likely to be classified as high-risk systems if they manipulate user behavior or threaten fundamental rights. Specifically, Point 1 of Annex III in the AI Act targets biometric tracking and emotion detection tools used within avatar ecosystems. At the same time, Points 3 and 4 cover automated behavioral tracking used for educational or employment purposes. Both rules apply directly to automated, AI-driven interactions inside virtual worlds (Kusche, 2023; Lynskey & Lynskey, 2015). For these high-risk classifications, the Act mandates strict standards for data quality, algorithmic transparency, and human oversight. While this framework's compliance-by-design approach is commendable, its practical enforceability within decentralised, user-generated virtual environments remains highly challenging. To address these systemic gaps, the European Commission’s Web 4.0 and Virtual Worlds Strategy explicitly promotes open international standards and user-centric design to ensure that future virtual architectures remain transparent, rights-compliant, and interoperable (Jiordan, 2023; Alexandre de Streel, 2025).

Yet, a clear division persists between voluntary industry norms and statutory laws. Within the EU framework, technical standards drafted by industry groups lack independent legal force. They become legally binding only when the European Commission incorporates them into official compliance architectures. The European Commission achieves this transition by sending formal requests to technical groups. This action transforms voluntary guidelines into an official benchmark un-

der binding laws like the DMA. For developers of decentralised global platforms, this mechanism is crucial. It determines whether cross-platform identities or digital assets are legally compliant, directly shaping platform accountability (Perey, 2024). In light of these challenges, this study organises the main points of the analysis into a structured overview. Table 2 outlines the five core legal instruments, scopes, key provisions, and practical limitations of the current EU legal framework for virtual world interoperability.

TABLE 2: EU's regulatory framework limitations in the context of metaverse interoperability (Source: Researcher's own compilation based on secondary data)

INSTRUMENT	SCOPE	KEY PROVISIONS FOR METAVERSE INTEROPERABILITY	OPERATIONAL LIMITATIONS
GDPR (General Data Protection Regulation)	Horizontal data protection law applicable across sectors.	Defines user rights including data portability (Art. 20); requires informed consent (Art. 4(11), 6, 7); cross-border transfer mechanisms ensure consistent protections.	Data portability is narrowly defined; it fails to address avatar or virtual asset transfers and lacks metaverse-specific interoperability guidance.
DSA (Digital Services Act)	Regulates platform responsibilities and content moderation.	Tiered obligations for platforms (esp. VLOPs); algorithmic transparency; moderation accountability; applies to user-generated content.	Rules are not specific to metaverse platforms; remains untested for immersive or decentralised virtual environments.
DMA (Digital Markets Act)	Applies to designated "gatekeepers" to ensure fair	Requires vertical and horizontal interoperability (Art. 6); mandates access to platform data and functionalities;	Enforcement mechanisms and technical specifications still evolving; application to real-time, immersive

INSTRUMENT	SCOPE	KEY PROVISIONS FOR METAVERSE INTEROPERABILITY	OPERATIONAL LIMITATIONS
	competition.	prevents infrastructure self-preferencing.	metaverse environments remains ambiguous.
Artificial Intelligence Act (AI Act)	Regulates AI systems based on risk categories.	High-risk AI systems (e.g., avatars, emotion detection) subject to strict compliance rules.	Applicability to decentralised metaverse settings uncertain; lacks metaverse-tailored enforcement mechanisms.
Data Governance Act (DGA)	Facilitates voluntary data sharing and governance.	Encourages trusted data intermediaries and data altruism while supporting technical data interoperability.	Participation is voluntary and interoperability remains limited by sectoral fragmentation.

Section 3. India's legal and policy landscape

India's legal and regulatory approach to virtual environments has evolved through a layered and gradual process. Initial regulatory efforts were shaped by the Information Technology (IT) Act 2000, which focused primarily on electronic records, digital signatures, and baseline intermediary liability (Fatima, 2023). Supplementary frameworks, such as the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, subsequently established early data security foundations and specific requirements for handling sensitive personal data (Seth, 2021). However, the scope of these early privacy rules remained strictly sectoral and fragmented. Conspicuously, the IT Act completely lacked explicit provisions capable of addressing the distinct, real-time demands of interoperable virtual worlds (B. Gupta & Mangal, 2024).

Over time, India's regulatory focus shifted toward asserting sovereignty over its digital ecosystem, increasingly treating data as a national asset (DAHRD, 2025). Driven by concerns regarding external surveillance and foreign control over critical digital infrastructure, subsequent state policies emphasised domestic data storage and conditioned cross-border data transfers (Thomas, 2019). This strategic evolution resulted in the enactment of the Digital Personal Data Protection (DPDP) Act 2023, which established a comprehensive statutory framework grounded in the constitutional recognition of privacy as a fundamental right (Justice K.S. Puttaswamy v. Union of India, 2017). The DPDP Act introduces the distinct legal category of the 'data fiduciary,' allocating clear statutory obligations to entities determining the purpose and means of data processing (Burman, 2020). Although the law secures basic user rights such as access, correction, and erasure, it fails to pro-

vide a technical roadmap for data portability. Additionally, the DPDP Act avoids the EU's strict adequacy rules, choosing instead to let the central government restrict or allow international data flows directly. India balances this state authority by promoting regulatory sandboxes. These tools enable platforms to test emerging technical models within supervised and safe environments.

However, while this sandbox approach enables technological experimentation, it remains largely disconnected from comprehensive legal reform. There is little coordination between these pilot policies and the systematic development of rules for metaverse interoperability, avatar governance, or user-generated assets (Panda Law, 2024). Since national policy focuses primarily on broad data-handling rules, very little regulatory attention has been paid to the specific infrastructure needs of immersive networks (Amlegals, 2024). Consequently, issues such as avatar portability, digital asset licensing, and cross-platform compatibility are completely absent from existing statutes (Kataria & Bothra, 2022). Currently, there are no laws in India that govern the transfer of avatars, virtual goods, or user profiles across competing ecosystems (Wadhwa, 2023). Similarly, domestic intellectual property laws have not been tailored to suit the unique nature of digital creations in immersive environments. As a result, rights related to ownership, licensing, and enforcement across platforms remain highly ambiguous, leaving users and software developers without legal certainty (Prasanna & Lavanya, 2023).

Section 4. Comparative analysis: EU vs. India

The legal gaps and structural differences highlighted in the previous sections show that the digital regulations of the European Union and India are moving along different yet parallel paths. While both systems are trying to address the challenges of automated systems and virtual worlds, they differ deeply in their legal approaches, oversight tools, and readiness to enforce open data sharing. This basic split directly determines whether either framework can successfully create a safe, open, and user-focused online environment.

Several key differences stand out when comparing India's approach with the EU model. First, the GDPR treats data privacy as a universal, fundamental right. In contrast, Indian law bases privacy on broader national goals like economic development and industry governance (Sinha, 2024). This basic split has major practical results for compatibility. The EU’s rights-first focus gives users active power to manage their online data, while India’s development-first model prioritises government flexibility over individual digital freedom. Second, the EU relies on an established, centralised oversight system, including the European Data Protection Board,

to ensure consistent enforcement across member states. In contrast, India's enforcement bodies are still under development (Labadie & Legner, 2023). This institutional delay creates severe challenges for platform compatibility. Without a strong, central enforcement authority, settling complex technical disagreements across different global platforms becomes extremely difficult, blocking cross-platform continuity.

Data portability forms a third key difference. The GDPR guarantees a user's right to extract and transfer data in a standard format, whereas Indian legislation lacks an equivalent statutory mandate. Crucially, missing technology-neutral standards critically limit how effectively users can manage their data (Pankhudi Khandelwal, 2024). We define these standards as rules targeting functional system compatibility instead of rigid platform code. This regulatory void allows platforms to exploit technical variations to lock users into proprietary systems. This statutory gap is further highlighted by how the two countries prioritise data principles. The GDPR specifically supports the active right to data portability. In contrast, the DPDP Act relies heavily on passive duties like purpose limitation and data minimisation (Nishith Desai Associates, 2025). These two approaches operate in a restrictive relationship. The EU framework attempts to help users securely move their data across competing platforms, while India's framework focuses on restricting how long a single company can keep user data. Consequently, India's heavy reliance on data deletion without a matching portability right actively blocks compatibility, as it forces data to be destroyed or siloed rather than safely transferred between platforms.

Finally, regarding platform governance, both regions place different duties on digital companies to manage international risks. The EU's DSA imposes tiered responsibilities depending on a company's market size. This approach helps secure fair algorithmic practices on very large platforms (European Commission, 2023). On the other hand, India's IT Rules center primarily on due diligence requirements and domestic complaint systems (MeitY, 2025). Additionally, both regulatory ecosystems consult different stakeholders to supplement their work. The EU has formalised such consultations in its Digital Strategy and Horizon Europe project, while India has been a slow follower and utilised the Telecom Regulatory Authority of India (TRAI) consultative papers and parliamentary standing committees to consult civil society, academia, and the private sector more regularly (Thierry Breton[2], 2022; TRAI, 2023).

Regulatory authorities in the EU, like the European Data Protection Board, have strong powers to investigate and punish violations. This includes the ability to is-

sue fines equal to four percent of a company's global yearly revenue (DPM, 2025). In contrast, India's newly formed Data Protection Board has no matching enforcement history. This gap raises serious doubts about its independence and overall ability to handle violations (Balakrishnan, 2025). This institutional divide also shows up in how each region handles core software systems. The EU's DMA forces dominant platforms to actively share data, allowing outside systems to connect with their software interfaces, user profiles, and messaging tools (Rowe, 2022). The Indian system handles this very differently, as the Competition Commission of India only checks for market abuse on a slow, case-by-case basis (PIB, 2022). International data flows represent another critical division affecting system compatibility. While the GDPR permits transfers only to nations offering adequate protections or under strict contractual safeguards (Kaya & Shahid, 2025), Section 16 of the DPDP Act empowers the Indian government to specify permitted destinations directly. This selective model faces academic criticism for prioritising state policy over a rights-based framework, which risks causing market fragmentation for international services (Narain, 2024). In virtual settings that require constant, real-time data exchanges, these mismatched legal structures pose severe barriers to regulatory compliance and enforcement (Frosio & Obafemi, 2025).

A major shared regulatory vacuum centers on user avatars. Neither the GDPR nor the DPDP Act explicitly recognise digital personas, virtual behavior tracking, or immersive harms. Instead, both frameworks govern these elements under general, legacy data protection rules. The EU AI Act addresses this gap by placing strict compliance rules on high-risk software, particularly tools tracking biometrics or human emotions. In contrast, India currently lacks any matching algorithmic laws. The lack of clear human control and explanation in automated choices inside virtual worlds risks violating basic user rights, leaving both developers and users in an environment of deep legal confusion (Tiwari, 2025).

To resolve this confusion, digital policy must decide whether an avatar should be legally classified as a data object or a legal subject. For example, consider a user in Frankfurt who builds a verified avatar on Meta Horizon Worlds, gathering a profile of her online behavior, virtual property, and a voice profile. She tries to transfer this entire avatar to an Indian virtual platform, TechMVerse, operated from Bangalore. Under EU law, her data portability right only covers the information she personally provided. It excludes the automated behavior insights generated by Meta. Furthermore, the Indian platform has no legal duty to accept her profile under the DPDP Act. Because no cross-border data agreement exists, her avatar effectively dissolves at the border. It remains trapped across two separate systems that fail to

recognize her digital identity.

If treated merely as a data object, an avatar is governed under broad personal data rules, reducing its identity traits, virtual assets, and behavior logs to commercial digital assets managed by a platform. Additionally, treating the avatar as an extension of a natural person's personality rights establishes it as a legal subject. This study argues that virtual world interoperability requires a dual framework. Avatars must be legally recognised as personality-rights-bearing extensions of natural persons to protect against identity theft, biometric manipulation, and emotional harm across platforms. At the same time, the underlying digital components of the avatar, such as its tokenised clothing, accessories, and portable metadata, should be regulated as separate legal objects. This will help users request cross-platform trade, licensing, and asset portability. Without this clear legal distinction, platform operators can easily exploit regulatory ambiguity to claim ownership over a user's digital persona, locking individuals into closed proprietary networks.

To address these systemic gaps, India can utilise the EU's structured, risk-based rules to strengthen its domestic framework. For instance, basic user safety could be woven into the DPDP Act by introducing data risk assessments and algorithmic transparency requirements for digital platforms. Furthermore, India can expand the foundational concept of data protection by design found in GDPR Article 25. By growing this narrow privacy rule into a broader compliance-by-design mandate, the state can legally compel software developers to build system compatibility and automated transparency tools directly into their early designs. Future legislation must provide clear legal recognition for user avatars. This step is necessary to establish procedural protections against digital impersonation, behavior manipulation, and virtual harms (Greenleaf, 2023). Rather than blindly copying European rules, India can use its existing regulatory sandboxes to develop a unique, hybrid regulatory model. This hybrid model is an adaptive framework. It blends the EU's strict, rights-centered corporate rules with India's flexible, market-led testing environments. Unlike traditional co-regulatory models that rely on voluntary industry self-governance supplemented by state oversight, this hybrid architecture makes user rights non-negotiable. Practically, this arrangement allows platforms to test new software architectures under state supervision while remaining bound by mandatory user-safety rules. This model bridges the classic divide between rigid statutory laws and private software innovation, ensuring that consumer protections do not block technical innovation.

Additionally, since virtual worlds function as borderless networks, both countries can explore a co-regulatory model of international harmonisation. This model

does not demand identical, uniform laws across borders. Instead, it relies on the mutual legal recognition of shared open technical standards and compatible data governance rules. Existing international treaties prove that this model is highly practical. For example, Singapore's international digital economy agreements with Australia, New Zealand, and the UK establish a system where separate nations officially accept each other's online user verification rules. Instead of rewriting their local privacy laws to match, the participating governments use shared software blueprints to securely verify a user's identity across borders (Digital Cooperation Organization, 2024). This collaborative setup enables citizens to access services and transfer digital profiles safely between different countries while complying with their own domestic regulations. This collaborative approach is essential to prevent global digital markets from fracturing into isolated national silos. By establishing a shared baseline for cross-platform data flows and secure identity verification, a co-regulatory framework allows independent networks to remain open, accessible, and safe. While India and the EU have advanced their digital market oversight, achieving true system compatibility requires moving past isolated national laws toward unified, cross-border legal foresight.

Conclusion and policy recommendations

International cooperation in metaverse governance is not merely a logistical convenience; it is a normative imperative grounded in the nature of virtual environments themselves. User avatars, data, and digital assets span multiple national borders and corporate networks simultaneously. Isolated national laws do not just complicate compliance; they actively weaken basic user rights across platforms. Users in jurisdictions with weaker protections bear the costs of interoperability without its safeguards, while platforms exploit divergence to route data through the path of least legal resistance. Harmonisation, in this context, does not mean erasing legal differences or forcing one region's values onto another. Instead, it means establishing a shared floor of user rights centered on avatar sovereignty, data portability, and cross-platform accountability. This reflects the foundational principle that certain user protections must follow persons into digital spaces, regardless of the jurisdiction in which a platform is incorporated.

This study highlights that while both the EU and India have established robust digital regulatory frameworks, neither has yet addressed the specific legal and institutional challenges presented by the metaverse. Even though the EU has a better legal and regulatory framework, critical issues such as avatar identity, portability of digital assets, and enforcement across virtual platforms remain unfathomed.

Although India has taken steps by replacing its earlier legal framework with the DPDP Act, several areas, such as virtual property, cross-border data rights, and platform obligations, still need legal clarity and operational depth. Hence, it is safe to surmise that neither system is sufficient on its own. Achieving secure and open virtual world compatibility requires a unified solution. This is where the policy directions for the already proposed hybrid regulatory model are needed. The model is a policy-oriented approach embedding the EU's rights-focused accountability standards into India's flexible, sandbox-driven testing environments, rather than a rigid technical framework.

To put this model into practice, five core policy changes are needed. *First and foremost*, legal frameworks in both India and the EU must explicitly recognise avatars as digital identities and protect them from impersonation, manipulation, and misuse. Lack of such norms will render its users and developers in a legal grey zone, vulnerable to disputes with little recourse. *Secondly*, endorsing a platform interoperability legal framework is essential to ensure openness and innovation in virtual ecosystems. Legal provisions that permit data portability and cross-platform compatibility would help resolve structural barriers and promote user autonomy. *Thirdly*, the success of any regulatory model depends considerably on the strength of its institutional infrastructure; India's Data Protection Board must be empowered with greater independence and operational clarity to effectively monitor compliance and provide recourse. *Fourth*, aligning legal and technical standards is vital; regulators must actively collaborate with industry leaders, civil society, and technical experts to ensure that ensuing standards for identity verification, secure data exchange, and user control are rooted in legal norms. *Fifth*, both jurisdictions should explore experimental and adaptive regulations such as regulatory sandboxes and pilot programs to test the feasibility of new legal frameworks before their implementation. These mechanisms allow regulators to work in collaboration with developers, isolating risks and finding solutions without stifling innovation. Additionally, empirical studies, analysing user and developer experiences, can form a foundation for regulatory tools that are both context-sensitive and globally relevant. Finally, continued investment in comparative legal research and empirical evaluation is the need of the hour to regulate shared public places like the metaverse. Future research must confer with key stakeholders like governments, academic institutions, and international bodies to assess how existing laws perform in actual metaverse settings.

References

Afzal, J. (2024). Legal challenges regarding digital operations. In J. Afzal (Ed.), *Implementation of digital law as a legal tool in the current digital era* (pp. 23–45). Springer Nature. https://doi.org/10.1007/978-981-97-7106-6_2

amlegals. (2024, May 29). Data localization in India: Implications for businesses and data security. *Amlegals Strategic Lawyering*. https://amlegals.com/data-localization-in-india-implications-for-businesses-and-data-security/

Archer, M., Ravn, L., & Thylstrup, N. B. (2025). The political economy of platformed silos: Theorizing data storage reconfigurations in the age of interoperability capitalism. *Big Data & Society*, *12*(2). https://doi.org/10.1177/20539517241303144

Balakrishnan, A. (2025, July 4). Enforcement gaps in India's DPDP Act and the case for decentralized data protection boards. *Express Computer*. https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140/

Bassini, M., Maggiolino, M., & De Streel, A. (2026, June 21). *Better law-making and evaluation for the EU digital rulebook*. CERRE. https://cerre.eu/publications/better-law-making-and-evaluation-for-the-eu-digital-rulebook/

Basu, A. (2022). India's engagement with global trade regimes on cross-border data flows. In Centre for Law & Policy Research (Ed.), *The philosophy and law of information regulation in India*. Centre for Law & Policy Research. https://publications.clpr.org.in/the-philosophy-and-law-of-information-regulation-in-india/chapter/indias-engagement-with-global-trade-regimes-on-cross-border-data-flows/

Bhatia, G. (2014). State surveillance and the right to privacy in India: A constitutional biography. *National Law School of India Review*, *26*(2), 127–158.

Bourreau, M. (2022). *DMA: Horizontal and vertical interoperability obligations*. Centre on Regulation in Europe. https://cerre.eu/wp-content/uploads/2022/11/DMA_HorizontalandVerticalInteroperability.pdf

Bradford, A. (2020). The Brussels effect. In A. Bradford (Ed.), *The Brussels effect: How the European Union rules the world* (pp. 25–66). Oxford University Press. https://doi.org/10.1093/oso/9780190088583.003.0003

Breton, T. (2022, September 14). People, technologies & infrastructure – Europe's plan to thrive in the metaverse [European Commission]. *Blog of Commissioner Thierry Breton*. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5525

Brownsword, R. (2024). *The future of governance: A radical introduction to law*. Taylor & Francis.

Burman, A. (2020). *Will India's proposed data protection law protect privacy and promote growth?* Carnegie India. https://carnegieendowment.org/files/Burman_Data_Privacy.pdf

Casanovas, P., de Koker, L., & Hashmi, M. (2022). Law, socio-legal governance, the internet of things, and industry 4.0: A middle-out/inside-out approach. *J*, *5*(1), Article 1. https://doi.org/10.3390/j5010005

Chen, H., Duan, H., Abdallah, M., Zhu, Y., Wen, Y., Saddik, A. E., & Cai, W. (2023). Web3 metaverse: State-of-the-art and vision. *ACM Transactions on Multimedia Computing, Communications and*

Applications, *20*(4), 1–42. https://doi.org/10.1145/3630258

Communication and IT Ministry. (2011). *The Information Technology Rules, 2011*. PRS Legislative Research. https://prsindia.org/billtrack/the-information-technology-rules-2011

DAHRD. (2025). India's data protection regime: Weak enforcement & government overreach. *Diaspora in Action for Human Rights and Democracy*. https://dahrd.org/2025/03/03/dpdpr_critique

Dhapte, A. (2026). *Europe metaverse market trends analysis report*. Market Research Future. https://www.marketresearchfuture.com/reports/europe-metaverse-market-60649

Digital Cooperation Organization. (2024). *Enabling cross-border data flows amongst the Digital Cooperation Organization member states*. Digital Cooperation Organization. https://dco.org/wp-content/uploads/2024/10/Enabling-Cross-Border-Data-Flows-Amongst-the-Digital-Cooperation-Organization-Member-States.pdf

DLA PIPER. (2025, June 26). *Data protection laws of the world – Enforcement in Germany*. DLA PIPER. https://www.dlapiperdataprotection.com/?t=enforcement&c=DE

DPM. (2025, March 3). 20 biggest GDPR fines so far [2025]. *Data Privacy Manager*. https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

Duggal, A., Gupta, D., & Gupta, M. (2023). Significance of NFT avtaars [sic] in metaverse and their promotion: Case study. *Scientific Journal of Metaverse and Blockchain Technologies*, *1*(1), 28–36. https://doi.org/10.36676/sjmbt.v1i1.04

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Eltanbouly, S., Halabi, O., & Qadir, J. (2025). Avatar privacy challenges in the metaverse: A comprehensive review and future directions. *International Journal of Human-Computer Interaction*, *41*(4), 1967–1984. https://doi.org/10.1080/10447318.2024.2374091

European Commission. (2021, April 21). *Proposal for a regulation laying down harmonised rules on artificial intelligence*. European Commission. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

European Commission. (2023a, April 25). *Digital Services Act: Very large online platforms and search engines* [Text]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

European Commission. (2023b, July 5). *An EU initiative on virtual worlds: A head start in the next technological transition*. European Commission. https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition

European Commission. (2023c, July 11). *Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds*. European Commission. https://digital-strategy.ec.europa.eu/en/news/towards-next-technological-transition-commission-presents-eu-strategy-lead-web-40-and-virtual

European Parliament and Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of*

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Official Journal of the European Union. http://data.europa.eu/eli/reg/2016/679/oj

European Parliament and Council. (2024). *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. Official Journal of the European Union. http://data.europa.eu/eli/reg/2024/1183/oj

Fatima, T. (2023). *Information technology law in India*. Kluwer Law International. https://www.torrossa.com/it/resources/an/5629139

Frosio, G., & Obafemi, F. (2025). Augmented accountability: Data access in the metaverse. *Computer Law & Security Review*, *59*, 106196. https://doi.org/10.1016/j.clsr.2025.106196

Garon, J. M. (2022). Legal implications of a ubiquitous metaverse and a Web3 future. *Marquette Law Review*, *106*, 163–242.

Geradin, D. (2021). *What is a digital gatekeeper? Which platforms should be captured by the EC proposal for a Digital Market Act?* (SSRN Scholarly Paper No. 3788152). Social Science Research Network. https://doi.org/10.2139/ssrn.3788152

Giacalone, M., & Arnone, G. (2024). Dispute resolutions for digital assets in a decentralized virtual world. *European Journal of Privacy Law & Technologies*, *1*, 117–135.

Gowda, T. (2025). *The synergy of metaverse, NFTs, and DeFi*. Educohack Press.

Graef, I. (2019). *Rethinking the essential facilities doctrine for the EU digital economy* (SSRN Scholarly Paper No. 3371457). Social Science Research Network. https://doi.org/10.2139/ssrn.3371457

Greenleaf, G. (2023). *Global data privacy laws 2023: 162 national laws and 20 bills* (SSRN Scholarly Paper No. 4426146). Social Science Research Network. https://doi.org/10.2139/ssrn.4426146

Grüner, A., Mühle, A., & Meinel, C. (2021). *Analyzing interoperability and portability concepts for self-sovereign identity*. 587–597. https://doi.org/10.1109/TrustCom53373.2021.00089

Gstrein, O. J., & Zwitter, A. J. (2021). Extraterritorial application of the GDPR: Promoting European values or power? *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1576

Guhathakurta, A. (2024). *Data privacy, data protection and user rights in the world of metaverse: Addressing the legal challenges in the EU, the US and India* (SSRN Scholarly Paper No. 4994031). Social Science Research Network. https://doi.org/10.2139/ssrn.4994031

Gupta, A., & Munde, S. (2025). *India metaverse market*. Market Research Future. https://www.marketresearchfuture.com/reports/india-metaverse-market-21443

Gupta, B., & Mangal, A. (2024). *Metaverse & privacy: Navigating legal and security concerns under data protection regulations* (SSRN Scholarly Paper No. 4728595). Social Science Research Network. https://doi.org/10.2139/ssrn.4728595

Gupta, M. (2025). Proposal to supercell: Integrating web 3.0 NFT-based avatars to unlock new revenue streams in clash of clans. *Scientific Journal of Metaverse and Blockchain Technologies*, *3*(1), 63–70. https://doi.org/10.36676/sjmbt.v3.i1.61

Hatami, M., Qu, Q., Chen, Y., Kholidy, H., Blasch, E., & Ardiles-Cruz, E. (2024). A survey of the real-time metaverse: Challenges and opportunities. *Future Internet*, *16*(10), Article 10. https://doi.org/1

0.3390/fi16100379

Hey, F. (2024). *Data interoperability and portability in the DMA: Competition booster or lame duck?* Technological University Ilmenau, Institute of Economics. https://www.tu-ilmenau.de/fileadmin/Bereiche/WM/wth/Diskussionspapier_Nr_192.pdf

Huber, L. (2025). Data interoperability and the governance of public value. *Platforms & Society*, *2*, 29768624251358686. https://doi.org/10.1177/29768624251358686

IBA Intellectual Property, Communications and Technology Law Committee. (2024). *Digital regulations in the metaverse era: India*. IBA Intellectual Property, Communications and Technology Law Committee. https://www.ibanet.org/document?id=Metaverse-project-India#:~:text=Are%20there%20any%20upcoming%20policies,a%20range%20of%20cyber%20threats.

International Centre for Law & Economics. (2025, June 26). *Digital competition regulations around the world*. International Center for Law & Economics. https://laweconcenter.org/spotlights/digital-competition-regulations-around-the-world/

Jacqueline Rowe. (2022, July 14). The EU Digital Markets Act: Is interoperability the way forward? *Global Partners Digital*. https://www.gp-digital.org/the-eu-digital-markets-act-is-interoperability-the-way-forward/

Jayakrishnan, M. (2024). The normalization of metaverse and the myth of data privacy. *International Journal of Computer Science Trends and Technology*, *12*(5), 27–32.

Jena, J. (2018). The impact of GDPR on U.S. businesses: Key considerations for compliance. *International Journal of Computer Engineering & Technology*, *9*, 309–319.

jriordon. (2023, April 17). Metaverse Standards Forum incorporates. *Metaverse Standards Forum*. https://metaverse-standards.org/news/press-releases/metaverse-standards-forum-incorporates/

Justice K.S. Puttaswamy (Retd) vs Union of India, Indiankanoon ___ (Supreme Court of India 2018).

Kaya, M., & Shahid, H. (2025). Cross-border data flows and digital sovereignty: Legal dilemmas in transnational governance. *Interdisciplinary Studies in Society, Law, and Politics*, *4*, 219–233. https://doi.org/10.61838/kman.isslp.4.2.20

Kowalski, A., & Nowak, T. (2023). Digital asset ownership in the context of virtual reality: Legal and ethical considerations. *Legal Studies in Digital Age*, *2*(4), Article 4.

Krishnamurthy, R. (2025, January 15). *Draft Digital Personal Data Protection Rules 2025 will only be a nominal checkbox: Apar Gupta*. Down To Earth. https://www.downtoearth.org.in/science-technology/draft-digital-personal-data-protection-rules-2025-will-only-be-a-nominal-checkbox-apar-gupta

Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI act: Fundamental rights and risk. *Journal of Risk Research*, 1–14. https://doi.org/10.1080/13669877.2024.2350720

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, *38*(1), 16–44. https://doi.org/10.1177/02683962221141456

Laborde, R., Ferreira, A., Lepore, C., Benzekri, A., Kandi, M. A., & Sibilla, M. (2023). The interplay between policy and technology in metaverses: Towards seamless avatar interoperability using self-sovereign identity. *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, 418–422. https://doi.org/10.1109/MetaCom57706.2023.00080

Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

Mäihäniemi, B. (2025). Enhancing autonomy of online users in the Digital Markets Act. In A. Engel, X. Groussot, & G. T. Petursson (Eds), *New directions in digitalisation: Perspectives from EU competition law and the charter of fundamental rights* (pp. 165–186). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65381-0_9

Martini, M. (2025). Materializing corporate futures: How the EU navigated the metaverse hype. *Information, Communication & Society*, *28*(5), 852–869. https://doi.org/10.1080/1369118X.2024.2428331

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). *A survey on decentralized identifiers and verifiable credentials*. arXiv. https://doi.org/10.1109/COMST.2025.3543197

MeItY. (2025, October 23). *Centre notifies amendments to IT Rules, 2021 to enhance transparency, accountability*. DD News. https://ddnews.gov.in/en/centre-notifies-amendments-to-it-rules-2021-to-enhance-transparency-accountability/

Metaverse Standards Forum. (2025, November 16). *The Metaverse Standards Forum*. Metaverse Standards Forum. https://metaverse-standards.org/

Narain, A. (2024, July 10). Cross border data transfers under the DPDP Act. *Leegality*. https://www.leegality.com/consent-blog/cross-border-data-transfer

Nath, S. N. S. (2025). Cross-border data transfer under Indian data protection regimes with special reference to the Digital Personal Data Protection Act, 2023. *Journal of Information Systems Engineering and Management*, *10*(3), 601–620. https://doi.org/10.52783/jisem.v10i3.5949

Nishith Desai Associates. (2025, November 19). *A new dawn: India's new data protection regime finally takes flight*. Technology Law Analysis. https://nishithdesai.com/research-and-articles/hotline/technology-law-analysis/a-new-dawn-indias-new-data-protection-regime-finally-takes-flight-15473

OECD. (2026). *An overview of national strategies and policies for immersive technologies*. OECD Digital Economy Papers. https://doi.org/10.1787/2da1d7da-en

OECD & Korea Development Institute. (2021). *Case studies on the regulatory challenges raised by innovation and the regulatory responses*. OECD Publications. https://doi.org/10.1787/8fa190b5-en

Panchal, S. (2024). *Cross-border data protection laws in India and European Union: A critical analysis of the complexities and the legal challenges* (SSRN Scholarly Paper No. 4970259). Social Science Research Network. https://doi.org/10.2139/ssrn.4970259

Panda Law, & Colors of India. (2025). *Suggestions for the TRAI 5G policy pertaining to questions about the metaverse & Web3 technology*. Telecom Regulatory Authority of India. https://www.trai.gov.in/sites/default/files/2024-11/COI_23012024.pdf

Pankhudi Khandelwal. (2024, November 27). The story of data portability in India: A lack of clarity under data protection, competition law and other frameworks. *Law School Policy Review*. https://lawschoolpolicyreview.com/2024/11/27/the-story-of-data-portability-in-india-a-lack-of-clarity-under-data-protection-competition-law-and-other-frameworks/

Perey, C. (2024). Interoperability is a fundamental requirement for the open metaverse. *2024 IEEE International Symposium on Emerging Metaverse (ISEMV)*, 21–24. https://doi.org/10.1109/ISEMV63338.2024.00019

PIB Delhi. (2022, October 20). *CCI imposes a monetary penalty of Rs. 1337.76 crore on Google for anti-competitive practices in relation to Android mobile devices*. Press Information Bureau. https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1869748

PIB Delhi. (2023, June 22). *TRAI releases consultation paper on 'Encouraging innovative technologies, services, use cases, and buisness models through regulatory sandbox in digital communication sector'*. Press Information Bureau. https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1934583

Prasanna, S., & Lavanya, P. (2023). Navigating the digital age: Challenges in Indian intellectual property rights law. *ILE Lawletter*, *1*(1), 34–44.

Prashant Kataria & Dhaval Bothra. (2022, May 23). *Metaverse: Legality & regulatory concerns In India*. Mondaq. https://www.mondaq.com/india/fin-tech/1195182/metaverse-legality-regulatory-concerns-in-india

Rawat, D. B., Alami, H. E., & Hagos, D. H. (2024). *Metaverse survey & tutorial: Exploring key requirements, technologies, standards, applications, challenges, and perspectives* (arXiv:2405.04718). arXiv. https://doi.org/10.48550/arXiv.2405.04718

Renieris, E. M. (2023). *Beyond data: Reclaiming human rights at the dawn of the metaverse*. MIT Press.

Rombolà, R. (2023, March 31). *Digital Markets Act and the interoperability requirement: Is data protection in danger?* MediaLaws. https://www.medialaws.eu/digital-markets-act-and-the-interoperability-requirement-is-data-protection-in-danger/

Seth, K. (2021). *India business guide 2022*. Seth Associates. https://www.sethassociates.com/wp-content/uploads/2022/02/India-Business-Guide_2022_ePUB-PDF.pdf

Sinha, S. (2024). Harmonizing data privacy laws: A comparative study of approaches in the EU, US and India. *Legal Spectrum Journal*, *4*, 1–59.

Sorrentino, G., & López-Guzmán, J. (2025). Rethinking privacy for avatars: Biometric and inferred data in the metaverse. *Frontiers in Virtual Reality*, *6*. https://doi.org/10.3389/frvir.2025.1520655

Strecker, J., Mayer, S., & Bektaş, K. (2025). *Towards societally beneficial personalized realities: A conceptual foundation for responsible ubiquitous personalization systems*. 1792–1814. https://doi.org/10.1145/3715336.3735709

Telecom Regulatory Authority of India. (2026, June 17). *The Indian Telecom Services yearly performance indicators 2024–2025*. Telecom Regulatory Authority of India. https://www.trai.gov.in/release-publication/reports/performance-indicators-reports

The London Story. (2025, June 17). *India's digital crossroads: Constitutional freedoms and the fight over platform regulation*. The London Story. https://thelondonstory.org/2025/06/17/indias-digital-crossroads-constitutional-freedoms-platform-regulation/

Thomas, P. N. (2019). *The politics of digital India: Between local compulsions and transnational pressures*. Oxford University Press.

Tiwari, S. (2025, July 26). *Towards rights-based AI framework in India: Bridging global models and constitutional duties*. LiveLaw. https://www.livelaw.in/lawschool/articles/towards-rights-based-ai-framework-india-bridging-global-models-constitutional-duties-298896

TRAI. (2023). *Digital transformation through 5G ecosystem* (Consultation paper). Telecom Regulatory Authority of India. https://www.trai.gov.in/sites/default/files/2024-11/CP_29092023.pdf

Trauttmansdorff, P. (2023). The fabrication of a necessary policy fiction: The interoperability 'solution' for biometric borders. *Critical Policy Studies*, *17*(3), 428–446. https://doi.org/10.1080/19460171.2022.2147851

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The Digital Services Act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*(1), 83–106. https://doi.org/10.1080/17579961.2023.2184136

Wadhwa, S., Doctorow, C., Dhruv, J., & Goyal, K. (2023, May 11). Securing privacy without monopoly in India: Juxtaposing interoperability with Indian data protection. *IJLT*. https://www.ijlt.in/post/securing-privacy-without-monopoly-in-india-juxtaposing-interoperability-with-indian-data-protection

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly*, *40*(4), 101873. https://doi.org/10.1016/j.giq.2023.101873

Wiewiórowski, W. R. (2025, June 13). *Shaping a safer digital future: A new strategy for a new decade*. European Data Protection Supervisor. https://www.edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future

Wolford, B. (2019, January 25). *What are the GDPR consent requirements?* GDPR.Eu. https://gdpr.eu/gdpr-consent-requirements/

Yang, L., Ni, S.-T., Wang, Y., Yu, A., Lee, J.-A., & Hui, P. (2024). *Interoperability of the metaverse: A digital ecosystem perspective review* (arXiv:2403.05205; Version 3). arXiv. https://doi.org/10.48550/arXiv.2403.05205

Published by

Alexander von Humboldt Institute for Internet and Society

CAIS Research for the Digital Age

in cooperation with

CREATe

cnrs centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies