INTERNET POLICY REVIEW

Volume 15 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Digital sovereignty and jurisdictional complexities in the metaverse: Rethinking legal authority in virtual spaces

Kasim Balarabe *O.P. Jindal Global University*

DOI: https://doi.org/10.14763/2026.3.2106

Published: 24 September 2026
Received: 14 November 2025 **Accepted:** 21 April 2026

Funding: The author 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: Balarabe, K. (2026). Digital sovereignty and jurisdictional complexities in the metaverse: Rethinking legal authority in virtual spaces. *Internet Policy Review*, *15*(3). https://doi.org/10.14763/2026.3.2106

Keywords: Metaverse governance, Digital sovereignty, Polycentric regulation, Virtual worlds, International technology law

Abstract: The metaverse disrupts long-settled allocations of legal authority by layering immersive virtual environments on top of distributed infrastructures that rarely map onto territory. This article argues that hierarchical, state-centric regulatory models cannot adequately govern such environments, because power is already distributed among states, platforms, protocol designers, and user communities. The article asks a precise legal question: how should legal authority be allocated across these actors to sustain rights, accountability, and coherence in immersive virtual worlds? To answer it, the article adopts a polycentric governance lens and develops a layered allocation-of-functions framework that distinguishes four governance layers (state law, platform governance, protocol architecture, and user and community norms) and specifies their cooperative, conflictual, and fallback interfaces, evaluated through the metrics of legality, legitimacy, efficacy, and auditability. Drawing comparatively on the GDPR's cross-border enforcement architecture and on the wider literature on international law and cyberspace, including the Tallinn Manual process, the article identifies how multi-level governance can produce order without hierarchy. It concludes with calibrated near-term and medium-term reforms and a research agenda attentive to re-territorialisation pressures and Global South perspectives.

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 metaverse, understood here as a loosely connected set of immersive, persistent, and data-intensive digital environments, is no longer a speculative venture. It is already being built through the convergence of spatial computing, virtual economies, identity systems, and behavioural analytics (Fairfield, 2005; Huynh-The et al., 2023; Wang et al., 2023). Its construction is occurring within a regulatory landscape that is already strained by social media, transnational data flows, and the infrastructural dominance of private platforms (Bygrave, 2014; Gillespie, 2018; Kuner, 2013; Lehdonvirta, 2022; Srnicek, 2016). The metaverse does not merely add to those pressures; it reorganises them, forcing a reconsideration of both territorial jurisdiction and the deeper assumptions that underlie the contemporary idea of digital sovereignty (Hörnle, 2021).

This article is therefore guided by a specific legal question: *how should legal authority over immersive virtual environments be allocated across states, platforms, protocol designers, and user communities so that the resulting order is coherent, legitimate, and capable of protecting rights across jurisdictions?* This question is not ornamental. It carries three analytical commitments that structure the argument. First, the question accepts the empirical premise that no single actor – not even the most assertive regulatory state – can unilaterally govern the metaverse. Secondly, it treats legal authority as genuinely distributed rather than as authority temporarily delegated by states to private actors. Thirdly, it insists that normative evaluation cannot be avoided: a distributed order still has to satisfy legality, legitimacy, efficacy, and auditability if it is to count as governance at all.

The central argument proceeds in three steps. First, the metaverse cannot be governed effectively through hierarchical, state-centric models because its architectures and institutional relationships are already polycentric, distributed among states, platforms, protocol designers, and user communities (Aguerre et al., 2024; De Filippi & Wright, 2018; Gorwa, 2019; Li & Yang, 2024). Secondly, effective governance frameworks therefore require a layered order in which authority is shared, contested, and overlapping, yet capable of producing stability and legitimacy. Thirdly, that layered order must respond not only to centrifugal pressures of globalisation but also to the recent re-territorialisation of digital policy, in which states

are increasingly asserting jurisdictional and values-based demarcation from particular technology providers (Chander & Sun, 2023; Pohle & Thiel, 2020).

The article proceeds in six further sections. Section 2 sets out a working definition of the metaverse and identifies the technical and institutional features that distinguish it from earlier digital environments. Section 3 demarcates digital sovereignty and explains why sovereignty-like authority now operates across four, not three, sites. Section 4 develops polycentric governance as an analytical lens. Section 5 sets out the layered allocation-of-functions framework that is the article's principal conceptual contribution. Section 6 distils lessons from social media regulation, particularly the General Data Protection Regulation's (GDPR) cross-border enforcement architecture. Section 7 examines the strain that metaverse architectures place on public international law, including engagement with the Tallinn Manual process as the leading restatement of international law in cyberspace. The conclusion proposes calibrated near-term and medium-term reforms and a research agenda attentive to re-territorialisation and Global South perspectives.

Section 1. The metaverse: Working definition and distinguishing features

Issue and approach

The metaverse has moved from speculative concept to a live governance problem (Wang et al., 2023; Xynogalas & Leiser 2024). The difficulty is not merely that the metaverse introduces new technologies in the abstract, but that it reconfigures long-standing distributions of authority among states, firms, technical communities, and users (Aguerre et al., 2024; Gillespie, 2018; Lehdonvirta, 2022). States remain committed to territorial jurisdiction, but the architectures that underpin immersive virtual environments rarely map onto territory (Hörnle, 2021). Platform companies build and control the environments in which interactions take place (Gillespie, 2018). Protocol designers define the data flows and allocation rules that shape behaviour (De Filippi & Wright, 2018). Users operate across borders, sometimes anonymously, and sometimes through persistent identifiers that are more revealing than their physical passports (Fairfield, 2005; Lastowka & Hunter, 2004). The result is not an absence of authority but an overabundance of competing claims to it (Aguerre et al., 2024; Hörnle, 2021; Lastowka & Hunter, 2004).

A workable and literature-anchored definition, and the one adopted here, is that the metaverse refers to an interconnected set of immersive, persistent, and interoperable digital spaces in which users interact through embodied representations

such as avatars and in which economic, social, and cultural activities occur in real time (Porto & Foà, 2023). Three elements of that definition carry analytical weight for legal purposes. The first is *persistence*. Metaverse environments are designed to continue existing regardless of whether a particular user is logged in (Castronova, 2005). That persistence is not simply a technical feature. It is the foundation of property-like claims over virtual assets: because a virtual sword, a plot of virtual land, or an avatar-bound wearable continues to exist, to be owned, and to be traded independently of any single user session, it begins to behave legally in the same way as a tangible object that the law has long been prepared to recognise as property (Fairfield, 2022; Lastowka & Hunter, 2004). By 'virtual assets' the article means persistent digital objects, including tokens, items, land parcels, identities, and credentials, to which users assert exclusive control and transferability within, and increasingly across, platforms. The second is *embodiment*. Interactions occur through avatars and digital identities that increasingly track biometric or behavioural information, with important consequences for privacy, data protection, and conceptions of personhood in virtual spaces. The third element is *interoperability*, which remains more aspirational than real, but nonetheless frames the policy imagination. The European Commission's 2023 Communication on Web 4.0 and virtual worlds explicitly ties the development of metaverse ecosystems to open standards and cross-platform portability (European Commission, 2023).

These traits do not create an entirely new universe. They amplify longstanding governance challenges of digital platforms (Suzor, 2019). Yet the intensity and scale of immersion alter the stakes. Two sets of differences, technical and institutional, explain why conventional regulatory models struggle in this domain.

1. Technical differences

Unlike traditional web environments, the metaverse depends on real-time rendering, spatial computing, biometric tracking, and low-latency networks that collapse physical and digital cues (Xynogalas & Leiser, 2024). These features produce unprecedented data density. Eye-tracking, gait analysis, emotional inference, spatial mapping, and continuous sensor data become routine inputs for platform optimisation (Xynogalas & Leiser, 2024). Early regulatory analyses demonstrate the difficulty of applying the GDPR's principles of data minimisation and purpose limitation to systems designed around continuous behavioural capture (Xynogalas & Leiser, 2024). The Artificial Intelligence Act (AI Act) adds a second layer of complexity, particularly where avatar-based interactions rely on emotion recognition or biometric categorisation (Regulation (EU) 2024/1689, 2024).

2. Institutional differences

The metaverse redistributes authority beyond the familiar state–platform dichotomy that has structured much internet-governance scholarship. That dichotomy is itself a working simplification drawn primarily from liberal democratic contexts, in which public regulators confront large private platforms; it fits less comfortably with authoritarian states that internalise platform functions through state-linked providers, or with states in the Global South whose regulatory capacity is constrained by infrastructural dependence (Bradford, 2023; Chander & Sun, 2023; Jiang, 2024). Even where the dichotomy holds, however, it now under-describes the terrain. Platforms design the physics, economies, and social architectures of immersive worlds (Gillespie, 2018). Protocol designers embed governance rules at the data layer. States attempt to project jurisdiction extraterritorially, often relying on territorial anchors that do not meaningfully exist in virtual environments. User communities, meanwhile, generate durable normative orders of their own. Scholars of digital sovereignty have shown that sovereignty claims increasingly hinge on infrastructural rather than territorial control (Bradford, 2023). The metaverse accelerates this shift because control rests not on geography, but on servers, standards, identity systems, and code. As Wenlong Li and Dan Yang argue, data governance has already moved into a polycentric domain in which no single actor can achieve comprehensive control (Li & Yang, 2024). The metaverse makes that polycentricity visible: authority is fragmented across states, firms, technical communities, and user collectives, each exercising partial sovereignty over different layers.

Section 2. Digital sovereignty demarcated

Digital sovereignty has become a phrase that everyone uses yet few define clearly. Its appeal derives from conceptual elasticity and the anxiety it expresses about authority in a world mediated by private infrastructures. Sovereignty has always been about control over flows – of people, goods, or information. The digital age magnifies and redistributes this concern across new actors. States remain central, but platforms, protocol designers, and user communities now claim forms of authority that resemble sovereignty in their functional effects. This article identifies four principal sites of sovereignty-like authority: state digital sovereignty, platform sovereignty, protocol or data-layer sovereignty, and community sovereignty. The fourth is expanded here in response to the useful observation that informal user-community authority (which the layered framework in Section 5 treats as a distinct governance layer) also exhibits core features of sovereignty and should be acknowledged as such at the outset rather than only later.

State digital sovereignty

Governments articulate digital sovereignty differently. The EU emphasises strategic autonomy and fundamental rights (Broeders et al., 2023). China often aligns digital sovereignty with a more classical conception of cyber sovereignty, emphasising territorial control and non-interference (Shumin, 2022). The United States rarely uses the phrase explicitly, but much of its industrial and national security strategy reflects similar concerns about maintaining control over critical digital infrastructures (Bradford, 2023). All three articulations reflect an intuition that states wish to regulate data flows, assert jurisdiction over platforms, and shape digital architectures.

Territorial jurisdiction remains central, yet the internet has never sat comfortably within territorial boundaries (Hörnle, 2021). The metaverse intensifies this discomfort for three concrete reasons that go beyond those already familiar from non-immersive platforms. First, a single interaction in a metaverse environment routinely crosses more jurisdictional lines than a comparable interaction on a conventional website, because immersive experiences depend on synchronous multi-party presence: a user in Nairobi, another in Seoul, and a third in São Paulo can co-inhabit a virtual venue that is hosted on servers in Ireland, moderated by a team in California, and built on standards maintained by a transnational open-source community. Secondly, the continuous nature of embodied interaction turns each session into a dense, ongoing stream of biometric and behavioural data; regulatory obligations that depend on discrete acts of collection or publication do not easily fit. Thirdly, the spatial logic of virtual worlds generates new objects of regulation (avatars, virtual land, in-world conduct) that were never anticipated by the jurisdictional doctrines designed for territorial activity.

States therefore rely increasingly on extraterritorial regulatory techniques. Article 3 of the GDPR is the most prominent example, asserting jurisdiction based on user location rather than of servers (Regulation (EU) 2016/679, 2016). The Digital Services Act and Digital Markets Act extend similar logic into content moderation and competition law (Regulation (EU) 2022/1925, Regulation (EU) 2022/2065, 2022). This technique effectively exports domestic regulatory standards abroad, a phenomenon Bradford has theorised as the Brussels Effect (Bradford, 2020). Yet extraterritoriality has limits. Enforcement remains patchy, and very large platforms can resist or adapt in ways that dilute sovereign control (Gentile & Lynskey, 2022). State digital sovereignty thus exists, but never in a pure form: it is filtered through platform architectures, shaped by technical standards, and constrained by the political economy of global data flows. It operates within a polycentric domain rather

than a hierarchical one (Aguerre et al., 2024).

Platform sovereignty

Platforms often exercise sovereignty even when they do not use the word. They set rules of access, define behavioural norms, and enforce sanctions (Gillespie, 2018). In the metaverse, platforms design the physics of virtual environments, specifying collision rules, avatar movement, and scarcity of virtual goods (Castronova, 2005). These are not mere technical choices. They are governance decisions with distributive consequences. Suzor describes the phenomenon as a form of private constitutionalism, in which the platform's terms of service function as the basic law of the digital domain (Suzor, 2019). Platform sovereignty rests on infrastructural control over servers and identity systems, on normative power to enforce community standards (Gorwa, 2019), and on economic authority over virtual economies (Lehdonvirta & Castronova, 2014). Although it is not absolute, platforms increasingly act as rule-makers, adjudicators, and enforcers in ways that functionally resemble sovereignty without constitutional safeguards.

Protocol/data-layer sovereignty

A third locus of authority sits deeper. Protocols and standards define how data is structured, transmitted, and verified, embedding values and governance choices into the data layer (DeNardis, 2014; Lessig, 1999). Blockchain scholars recognised this early. De Filippi and Wright describe blockchain systems as architectures in which code implements governance rules, sometimes replacing or constraining legal authority (De Filippi & Wright, 2018). In the metaverse, data-layer sovereignty emerges through identity standards, interoperability protocols, cryptographic verification systems, and behavioural telemetry pipelines. These determine what can be tracked, what can be moved between platforms, and how users authenticate themselves. The power here is subtle but profound. A protocol can enable portability or prevent it; it can allow anonymity or require a persistent identity; it can make certain forms of surveillance technically unavoidable (Nissenbaum, 2005). This layer is itself highly polycentric: standards bodies, open-source communities, platform engineers, and, at times, governments all influence protocol design, yet no single entity controls it.

Community sovereignty

A fourth locus of sovereignty-like authority, often overlooked in state-centric accounts, is the sovereignty exercised by user and community collectives. Users establish social expectations, behavioural norms, and informal dispute-resolution

mechanisms that influence conduct inside virtual environments (Taylor, 2006). In immersive environments, user collectives develop rules around identity expression, acceptable conduct, stewardship of virtual property, and participatory governance. These norms lack formal status, yet they govern in the most immediate sense: they shape what people do, tolerate, and expect. Treating community authority as a fourth face of sovereignty is consistent with scholarship on indigenous data sovereignty, which insists that self-determination over data, systems, and shared cultural artefacts cannot be reduced either to state authority or to platform rule-making (Jiang, 2024; Kukutai & Taylor, 2016). The significance of this move is substantive rather than terminological: recognising community sovereignty prevents the layered framework developed below from treating user norms as merely the residue left after states, platforms, and protocols have acted.

Tensions and overlaps

When these four forms of sovereignty-like authority coexist, tensions are structurally inevitable rather than merely contingent. Interoperability standards can undermine data localisation; privacy-enhancing protocols could frustrate law enforcement (DeNardis, 2014); platform design can override community expectations; state demands for traceability can collide with community norms of pseudonymity. Sovereignty in the metaverse is multiplying, fragmenting, and reassembling across layers. Digital sovereignty becomes less a statement of control than a question about how control is distributed when no single actor can govern alone.

Section 3. Polycentric governance as an analytical lens

Polycentric governance, in its contemporary meaning, refers to systems in which authority is distributed across multiple centres of decision-making that operate at different levels, with varying degrees of formality, and without strict hierarchical ordering (Aguerre et al., 2024; Ostrom, 2010). Polycentricity is not a normative aspiration but an analytical recognition that real-world governance rarely operates through a single sovereign command. The digital environment is a vivid example, given the density of actors exercising authority over it. Three features are central.

Firstly, polycentric governance is *multi-level*. Authority is exercised simultaneously at the local, national, regional, and transnational levels. States regulate platforms; the European Union issues regulations with extraterritorial reach; global technical communities design standards; and user groups establish social norms (Aguerre et al., 2024). These levels do not align neatly. They intersect, overlap, and occasionally contradict one another. The metaverse amplifies this because its spatial logic

does not correspond to territorial jurisdiction.

Secondly, polycentric governance is *multi-actor*. States remain important, but they are not alone. Platforms exercise governance power through terms of service, algorithmic moderation, architectural design, and economic rules. Technical bodies define standards that determine interoperability, data formats, identity schemes, and security protocols (Gorwa, 2019). Civil society organisations, open-source communities, and user groups add normative layers, shaping expectations of fairness and legitimacy (Taylor, 2006). These actors do not operate within the same institutional logic. They also do not share the same interests or aims: regulators are typically oriented towards rights protection and public policy, platforms towards user growth and shareholder value, technical communities towards interoperability and technical integrity, and user groups towards expressive freedom and community well-being. Those divergent orientations produce predictable forms of friction, which the framework developed below is designed to accommodate rather than to suppress.

Thirdly, polycentric governance combines *formal and informal rule-making*. It includes hard law from legislatures and courts, but also soft law from regulators, non-binding guidelines, technical standards, platform policies, and the informal norms that emerge within user communities (Gillespie, 2018). Aguerre, Campbell-Verduyn, and Scholte show that informal sources of authority are not peripheral but structurally embedded in global digital governance (Aguerre et al., 2024).

These properties prevent any single actor from claiming comprehensive control. Polycentric governance is, in this respect, less a choice than a description of how authority is exercised once the fiction of a single sovereign centre is set aside.

Ordered pluralism rather than hierarchy

Polycentric governance rests on the insight that governance systems can be plural without being disorderly. The phrase 'ordered pluralism' captures this idea: multiple centres of authority coexist, coordinate, and sometimes compete, yet the overall system remains intelligible. This contrasts with hierarchy, which presupposes a clear chain of command. In digital governance, hierarchy fits poorly – no regulator, platform, standards body, or court can fully determine outcomes. Even the most ambitious regulatory projects rely on platforms to implement and interpret rules in practice (Gentile & Lynskey, 2022). Conversely, platform policies are shaped and constrained by legal and normative expectations from multiple jurisdictions, and standards bodies negotiate among divergent interests while incorporating political

pressures indirectly. None of these relationships is hierarchical in the classical sense.

Ordered pluralism, therefore, suggests a different conceptual architecture closer to a set of loosely coupled nodes interacting through mutual constraint than to a pyramid. Authority emerges relationally, through negotiation, contestation, and adaptation.

Why the metaverse is already polycentric

The metaverse is, by design, a polycentric governance environment. Four observations explain why, and together they suggest that polycentricity is more a structural entailment of the technology than a contingent policy choice. Firstly, doctrinally, the metaverse challenges territorial jurisdiction. International jurisdiction doctrines remain tied to physical location, effects, nationality, and control over infrastructure (Hörnle, 2021), yet immersive environments operate across distributed servers, virtual assets, and behavioural data that do not map onto territorial space. The jurisprudence on internet jurisdiction, from Yahoo! France to Google Spain ("*Google Spain SL v AEPD*," CJEU 2014), already shows the limits of territoriality. The metaverse intensifies this because its architectures do not contain natural territorial markers. Secondly, platform power is structurally embedded: platforms define identity systems, implement behavioural norms, and regulate virtual economies (Castronova, 2005). Platforms are co-governors, not merely subjects of regulation. Thirdly, protocol design operates as distinct governance. Protocols define data flows, interoperability, and security mechanisms, constraining states and platforms alike (De Filippi & Wright, 2018). Fourthly, practicality forces cooperation. No single actor possesses comprehensive capacity and polycentric systems require coordination (Ostrom, 2010). Taken together, these four considerations suggest that the polycentric character of metaverse governance is effectively unavoidable; the real question is whether it will be generated by design or by drift.

Section 4. A layered allocation-of-functions framework

If the metaverse is structurally polycentric, the next question is how to allocate governance functions among actors who share neither constitutional foundations nor a clear hierarchy. The framework developed in this section, and put forward as the article's principal conceptual contribution, builds on the polycentric premises established above. It does not assume the existence of a central sovereign. It instead identifies four discrete layers through which governance actually occurs, specifies the interfaces among them, and sets out metrics by which the perfor-

mance of each layer can be evaluated.

The four layers and their primary functions

The four layers (state law, platform governance, protocol architecture, and user/community norms) are conceptual categories that correspond to concrete institutional arrangements. The ordering is not hierarchical. It maps where authority actually sits. State law remains indispensable. It establishes the fundamental rights that underpin digital participation, provides enforcement mechanisms, and articulates public policies relating to safety, data protection, and competition. In the metaverse, state law includes privacy regulation such as the GDPR, consumer protection norms, intellectual property rules, and national criminal law. Its primary function is to articulate public-interest constraints that platforms and technical actors must respect and to express democratic values to private governance systems (Bradford, 2020).

Platform governance functions as the primary governor of the metaverse. Platforms design identity systems, define user conduct rules, mediate disputes, and construct economic architectures (Gillespie, 2018). Their governance tools range from automated moderation to algorithmic ranking, spatial design, access controls, and sanctions. Their primary function is operational rule-making: they determine how interactions occur in practice, which behaviours are permitted, and how conflicts are resolved (Gorwa et al., 2020).

Protocol architecture shapes what is technically possible. Standards-setting bodies, open-source communities, and infrastructure developers design protocols governing identity verification, interoperability, authentication, cryptographic functions, and data structures (Lehdonvirta, 2022). These architectures determine the default conditions of digital life. A protocol can enforce privacy by design, mandate interoperability, or limit data retention. Its primary function is constraint-setting. It defines the boundaries within which platforms and states must operate (De Filippi & Wright, 2018).

Finally, user/community norms constitute the layer that platforms and regulators can neither generate nor fully suppress. Users and communities establish social expectations, behavioural norms, and informal dispute-resolution mechanisms (Taylor, 2006). In immersive environments, user collectives develop rules around identity expression, acceptable conduct, virtual property stewardship, and participatory governance. Although such norms lack formal status, their primary function is legitimacy-generation: they provide meaning to the environment and shape

compliance through social incentives rather than coercion.

Interfaces: cooperation, conflict, and fallback

The four layers interact in three main ways: cooperation, conflict, and fallback. These interfaces create the dynamic texture of metaverse governance. Cooperation occurs when actors at different layers work toward aligned or mutually compatible outcomes. State law may encourage platforms to implement robust content-moderation procedures, as the Digital Services Act does. Platforms may adopt voluntary standards that complement regulatory goals. Protocol designers often cooperate with both regulators and platforms to embed rights-compliant features such as privacy-preserving computation or interoperability functions (Aguerre et al., 2024). User communities may cooperate with platforms through participatory governance schemes, co-authored norms, or collective decision-making. Cooperation is rarely perfect, but when it occurs, it produces regulatory coherence.

Conflict is equally common, and it is analytically important because the actors at different layers pursue different interests and aims. A state may mandate data localisation while platform architectures depend on global storage and replication (Hörnle, 2021). Protocol-level anonymity may conflict with state preferences for traceability and surveillance. Platform design choices may frustrate the objectives of state safety regulators or user communities; an avatar-based reporting mechanism may satisfy platform efficiency goals but fail to meet due-process or transparency expectations. Conflicts arise because layers have different incentive structures, different sources of legitimacy, and different epistemic commitments. These conflicts are not pathological. They are constitutive of polycentric systems.

Fallback mechanisms are triggered when one layer fails to perform its functions. If platform moderation collapses, states may intervene through emergency orders, mandatory audits, or injunctions. If state regulation is weak or absent, platforms or standards bodies may step in to protect user rights or manage harmful behaviours (Suzor, 2019). User communities may create their own governance infrastructures to fill gaps. Fallback arrangements prevent system-level collapse and reveal where responsibility ultimately resides in practice, even when formal competencies are ambiguous.

Success metrics: Legality, legitimacy, efficacy, auditability

Four metrics help assess whether each layer performs adequately. Legality refers to compliance with binding legal norms, especially fundamental rights, data protection rules, and jurisdictional limits (Lynskey, 2015). State law must be clear, pro-

portionate, and enforceable; platform rules must comply with public-law obligations; protocol designs must avoid creating architectures that undermine legal rights, such as unavoidable biometric tracking or opaque automated decision-making (European Data Protection Board, 2020).

Legitimacy concerns the moral authority of governance actions (Habermas, 1996). States derive legitimacy from democratic processes and public accountability (Beetham, 1991). Platforms derive it from consent, transparency, responsiveness, and fairness (Klonick, 2018). Protocol designers derive it from participatory processes, peer review, and technical integrity (DeNardis, 2014). User communities derive it from shared norms and collective decision-making (Ostrom, 1990). In a polycentric environment, legitimacy is multi-sourced (Ostrom, 2010).

Efficacy refers to the ability of a governance mechanism to produce desired outcomes. A legal rule may be legitimate and lawful, but ineffective if it cannot be enforced (Ostrom, 2010). Platform moderation systems may be efficient at scale but ineffective at addressing structural harms (Douek, 2021; Eder, 2024; Gillespie, 2018). Protocol-level interventions may be technically elegant, but practically unworkable if adoption is low. Efficacy, therefore, requires attention to feasibility, incentives, and resource constraints.

Auditability, finally, refers to the ability to inspect, verify, and understand governance processes. State regulators need auditability to enforce compliance (Husovec, 2023). Platforms need it to evaluate algorithmic systems and moderation outcomes. Technical communities need it to validate protocols. Users need it to build trust. In the metaverse, where automated decisions shape user experience continuously, auditability is essential for preventing opacity and unaccountable power.

Section 5. Lessons from social media governance

Social media is the first large-scale experiment in digital governance under conditions of transnationality, rapid scaling, and infrastructural dependency. The metaverse inherits this history even as it transforms the technological environment. Its lessons, though imperfect, confirm that governance in distributed systems requires coordination across layers, and failures at any one layer can destabilise the whole.

The GDPR's cross-border enforcement system exemplifies polycentric coordination. It operates through a structured network that includes national Data Protection Authorities (DPAs), a lead supervisory authority (LSA) for cross-border processing,

and the European Data Protection Board (EDPB) as the dispute-resolution and harmonisation body (Regulation (EU) 2016/679, 2016). Under the One-Stop-Shop (OSS) mechanism, cross-border cases are handled primarily by the DPA of the controller's main establishment, which acts as the lead supervisory authority; other concerned DPAs can raise objections, require modifications, or trigger EDPB intervention (Tosoni, 2020). The result is a system in which authority is shared and continually negotiated: no DPA can unilaterally impose a divergent interpretation of the GDPR, and the LSA cannot act without considering objections from other DPAs. The EDPB's binding decisions illustrate this dynamic. In high-profile cases against Meta (European Data Protection Board, 2022a, 2022b), WhatsApp (European Data Protection Board, 2022c), and TikTok (European Data Protection Board, 2023a), the Board intervened to resolve disputes over legal bases, transparency, and children's data. These were not mere procedural interventions. They clarified substantive obligations and ensured consistent application of EU law. This coordination is polycentric because authority is distributed among many actors, and yet order emerges through iterative negotiation and binding *ex post* harmonisation. The GDPR therefore, demonstrates that distributed governance can produce stable outcomes without collapsing into fragmentation, provided coordination mechanisms exist. Without the OSS and EDPB, enforcement would have resembled a patchwork of inconsistent decisions (Gentile & Lynskey, 2022).

The system's performance has nonetheless been uneven. Its successes cluster around cases involving controllers with a clear EU establishment, where layered coordination has worked reasonably well (Gentile & Lynskey, 2022). Three categories of failure nevertheless stand out. Controllers without EU establishment exposed a fundamental gap, leading to parallel investigations and inconsistent interpretations (European Data Protection Board, 2018). Article 66 urgency procedures, intended to allow provisional measures in urgent cases, have been invoked rarely; the 2023 Urgent Binding Decision ordering Meta to prohibit certain data processing (European Data Protection Board, 2023d) exposed tensions about how DPAs should interpret the 'serious and irreparable harm' threshold and about the interaction between urgency and the collective decision-making structure of the consistency mechanism (European Data Protection Board, 2023b). EDPB taskforces have produced some outcomes, such as coordinated cookie-banner guidance, but the voluntary model produces inconsistent implementation when national priorities differ (European Data Protection Board, 2021, 2023c). These failures show that polycentric governance needs clear escalation and decision-making mechanisms when actors disagree.

Transferability to immersive worlds

The social media lessons translate to the metaverse only in part. Some carry over directly, others require substantial adaptation, and a few break down entirely once the immersive setting is taken seriously. A stylised scenario clarifies what does and does not transfer.

Consider a cross-border avatar-harassment incident. A user resident in Spain alleges that another user, resident in Germany, subjected her avatar to repeated unwanted physical contact during a public event held inside a virtual venue operated by a platform whose European subsidiary is established in Ireland and whose identity layer is supplied by a third-party provider headquartered in the United States. Under the GDPR's One-Stop-Shop, the Irish DPA would assume the role of lead supervisory authority, while the Spanish DPA would be a concerned authority entitled to raise objections under the consistency mechanism, with EDPB intervention available in the event of disagreement (Regulation (EU) 2016/679, 2016, arts 56, 60–65; Tosoni, 2020). To that extent, the existing architecture works. Three difficulties, however, immediately surface. First, the conduct engages data-protection law, consumer-protection law, platform-liability rules, and potentially criminal law in more than one member state, and the One-Stop-Shop coordinates only the first of these. Secondly, the third-party identity provider may have no European establishment at all and would therefore fall outside the main-establishment rules, reproducing in sharper form the establishment-less-controller gap already familiar from social media enforcement (European Data Protection Board, 2018; Gentile & Lynskey, 2022). Thirdly, the evidential basis of any enforcement, namely biometric telemetry and spatial logs, is generated and held by the platform itself, and its reliability cannot be tested without the platform's cooperation (Xynogalas & Leiser, 2024).

Three lessons of social media governance nonetheless transfer with relatively little adjustment. The first is the value of structured, institutionalised coordination among regulators rather than reliance on ad hoc cross-border cooperation (Aguerre et al., 2024). The GDPR experience demonstrates that distributed authority can produce stable outcomes provided that a designated coordinating regulator, a duty of cooperation, and a binding dispute-resolution body are in place (Tosoni, 2020). The second is the necessity of *ex post* interpretive alignment through reasoned decisions, of the sort that the EDPB's binding decisions have produced in cases against Meta, WhatsApp, and TikTok (European Data Protection Board, 2022a, 2022c, 2023a). Without such a mechanism, divergent national interpretations would generate the patchwork that the One-Stop-Shop was designed to pre-

vent (Gentile & Lynskey, 2022). The third is that platforms and standards bodies routinely act as interim governors where formal regulatory capacity is lacking, and this redundancy across layers is a structural virtue of polycentric coordination rather than a defect to be eliminated (Gillespie, 2018). What is genuinely transferable is therefore not the One-Stop-Shop as such, but its institutional grammar.

That grammar can be reproduced for immersive environments only if a regional digital authority is taken seriously rather than gestured at as an aspiration. The EDPB supplies a useful template, but a metaverse counterpart would have to differ from it in four respects: cross-regime membership extending to consumer-protection, audiovisual-media, and competition regulators, with formal participation by Digital Services Coordinators (European Parliament and Council of the European Union, 2022b, art 49); jurisdictional reach attaching to the operation of immersive infrastructure accessible to residents of the regulating jurisdiction, extending to platform architecture the targeting logic of Article 3 GDPR (European Parliament and Council of the European Union, 2016, art 3); decisional procedures with permanent technical-advisory capacity, since many metaverse disputes turn on protocol behaviour and biometric inference rather than legal interpretation alone; and remedial powers including architectural orders capable of requiring the redesign of protocol-level features rather than confining the authority to fines and behavioural injunctions. The Digital Services Act's Digital Services Coordinators with EU-level oversight (Regulation (EU) 2022/2065, 2022) and the European Commission's Communication on Web 4.0 (European Commission, 2023) suggest that the legislative imagination already extends in this direction.

Three structural differences nonetheless limit transferability regardless of institutional design. Metaverse identity systems rely on biometric and behavioural data more intrusive than social media identifiers (Xynogalas & Leiser, 2024), shifting the centre of regulatory gravity from *ex post* moderation to *ex ante* protocol-level constraints on what data can be captured at all. The metaverse is also spatial and economic in ways that social media is not; virtual property and user-generated economies (Castronova, 2005) generate disputes that resemble those arising from financial markets and real-property regimes more than those arising from speech, making enforcement more dependent on platform design. And whereas social media platforms are largely siloed, the metaverse aspires, at least normatively, to interoperability across environments (European Commission, 2023), which disperses the locus of harm: an avatar that moves across platforms carries its identity, assets, and reputational record with it, so that a regulatory action against one platform may be circumvented through migration to another unless coordination operates

at the protocol layer.

Four adaptations follow. First, protocol-level harmonisation, particularly for identity, data minimisation, and portability, is structurally indispensable: without it, regulatory action remains downstream of the architecture that generates the relevant harms (De Filippi & Wright, 2018). Secondly, cross-platform enforcement agreements modelled loosely on the One-Stop-Shop must be extended across regimes and across the actor types canvassed above. Thirdly, technical-auditability requirements, including standardised logging of behavioural-telemetry processing, mandatory disclosure of biometric-inference pipelines, and verifiable audit trails for cross-platform identity transfers, are needed to address the evidential gap exposed in the avatar-harassment scenario (Gorwa et al., 2020). Fourthly, institutionalised cooperative oversight must bring together regulators, platforms, and standards bodies in a structured exchange in which protocol choices, legal requirements, and technical implementation are reciprocally accountable. None of these four adaptations is sufficient alone: protocol-level harmonisation without cross-platform enforcement leaves architectural standards unenforced; cross-platform enforcement without auditability cannot generate the evidence necessary for action; auditability without cooperative oversight produces technical compliance disconnected from regulatory purpose. The package is demanding rather than complete, and it leaves unresolved the question of how user communities, whose normative authority (community sovereignty section) identifies as a fourth site of sovereignty, are to participate in coordination structures designed primarily for regulators, platforms, and standards bodies. The social media experience provides a conceptual foundation, but the metaverse's technical and institutional complexity requires building on that foundation rather than replicating it.

Section 6. International law and state control under strain

International law has always assumed a world of borders, territories, and identifiable actors. It now confronts infrastructures that defy those assumptions. States still wish to exercise control, yet the doctrinal and enforcement mechanisms on which they rely are increasingly mismatched with the architectures they seek to regulate. Three dimensions of strain merit examination: traditional jurisdiction doctrines struggling under distributed architectures; conflicts between public regulatory norms and private rules; and evidential and remedial challenges.

Jurisdictional doctrines under distributed architectures

International law recognises several bases of jurisdiction, including territoriality, nationality, and protective principles (Shaw, 2021). Distributed architectures lack stable territorial anchors (Arner et al., 2022). A user in Nairobi may interact in a virtual concert hosted on servers in Ireland, moderated from California, and built on standards developed by a transnational open-source community that itself has no legal personality, that is, no status as a legal subject and therefore no capacity to sue or be sued as an entity, leaving liability to attach, if at all, to individual contributors or sponsoring foundations. Jurisdictional doctrines can adapt only so far: the territorial principle loses explanatory power when location is diffuse; effects doctrine risks overbreadth (Hörnle, 2021). What emerges is jurisdictional fragmentation: states assert overlapping claims, none fully enforceable without platform cooperation. International law must therefore integrate infrastructural considerations (Aguerre et al.,2024), and scholars such as Hörnle propose rethinking jurisdiction through functional and technical criteria, focusing on where control is exercised rather than where servers are located (Hörnle, 2021).

The most developed attempt to bring public international law to bear on cyberspace is the Tallinn Manual process. *Tallinn Manual 2.0*, produced by an international group of experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence and currently being succeeded by *Tallinn Manual 3.0*, sets out 154 rules restating international law as applicable to cyber operations in both peacetime and armed conflict, with extensive commentary on sovereignty, jurisdiction, state responsibility, human rights, and due diligence (Schmitt, 2017). The Manual is not formally binding; it represents the views of its authors in their personal capacity. Yet it is the most influential doctrinal reference point in the field, widely consulted by governments and scholars, and it supplies a useful touchstone for metaverse governance in two respects. First, its treatment of sovereignty and of the duty of due diligence establishes that cyber operations do not occur in a legal vacuum: the ordinary principles of international law apply, including the obligation not to allow one's territory or infrastructure to be used to harm other states. Secondly, the Manual's careful disaggregation of jurisdiction into prescriptive, adjudicative, and enforcement dimensions illustrates precisely the kind of functional analysis that metaverse governance requires. At the same time, the Manual remains premised on state-to-state relations and on the attribution of conduct to states; it has comparatively little to say about the role of private platforms and technical communities that the present framework places at the centre of immersive governance. Engagement with the Tallinn process, therefore, situates the argument within the broader debate on international law and digital infrastructures,

while clarifying why that debate must now be extended beyond inter-state conduct to capture polycentric authority.

Conflicts of laws and private ordering

A second source of strain arises from conflicts between public law and private ordering. Platforms and protocols create normative systems that operate parallel to, and sometimes in tension with, state-made law. Terms of Service (ToS) govern user conduct, define property rights, impose dispute-resolution procedures, and specify jurisdictional clauses (Moringiello, 2010). They often displace public remedies through arbitration mandates or liability disclaimers. In immersive environments, ToS can take on even greater significance because they govern spatial interactions, avatar rights, and the architectural logic of the world itself. Suzor describes this as a form of private constitutionalism, where platforms become primary lawmakers (Suzor, 2019).

Code adds a further dimension. Code enforces behavioural constraints automatically, from avatar movement to identity persistence and virtual property transfers (Gillespie, 2018). As De Filippi and Wright argue, code can become a regulatory mechanism in its own right, sometimes more powerful than contract or public law (De Filippi & Wright, 2018). Protocols can determine whether data is interoperable, whether anonymity is possible, or whether user actions are reversible. States may object, but unless they can compel technical redesign, their objections remain largely symbolic. These collisions between public and private norms are not theoretical. Consider a platform that enforces mandatory identity verification through persistent avatars. A state may consider such verification unlawful or disproportionate, yet the platform may embed it directly into the architecture. Consider, alternatively, a jurisdiction that recognises virtual property rights, while a platform treats all virtual assets as mere contractual licences. The conflict exists not merely in text but in the functioning of the system. Public and private orderings clash here not only because they apply different rules but because they pursue structurally different aims. Public law privileges accountability, fundamental rights, and democratic legitimacy; private orderings privilege user retention, transactional efficiency, and economic viability. These aims are not always reconcilable through interpretive adjustment, and the resulting collisions are therefore substantive rather than merely procedural. International law offers limited tools to mediate these tensions. Conflict-of-laws doctrines might determine the applicable law, but enforcement still depends on cooperation from private actors. Treaty regimes, such as those under UNCITRAL's electronic commerce frameworks, provide functional equivalence rules but do not address immersive interactions or avatar-based iden-

tities. The result is a regulatory asymmetry: public law aspires to universality, while private law follows the platform's infrastructural boundaries.

Evidential and remedial constraints: Why law still matters

A third area of strain concerns evidential and remedial challenges. Distributed architectures generate massive technical data, yet access is controlled by platforms (Xynogalas & Leiser 2024). Attribution is complicated when actions involve bots, avatars, or algorithmic agents; harmful acts may be products of systems rather than single users. Traditional remedies assume a clear defendant; in the metaverse, some harms may be architectural, requiring redesigning systems rather than punishing actors.

Despite these constraints, law provides normative anchors that private ordering cannot replace. Legal processes reinforce legitimacy, providing accountability that private governance lacks (Gentile & Lynskey, 2022). Law's most enduring contribution is the demand for justification. Law requires platforms and protocol designers to explain and defend their choices publicly – a crucial counterweight to unaccountable power in a polycentric environment.

Conclusion: Calibrated reforms and a research agenda

The metaverse is neither a clean break from past digital ecosystems nor simply an extension of them. It is more layered, more immersive, and more structurally polycentric. Governance in such environments requires calibrated reforms rather than maximalist interventions or unreflective reliance on private ordering. It also requires attentiveness to a counter-trend that cuts against the metaverse's inherent transnationality: a growing political appetite for re-territorialisation. In an international climate increasingly marked by geopolitical competition, industrial strategy, and value-based demarcation from particular technology providers, states are once again projecting territorial and civilisational boundaries into digital policy (Chander & Sun, 2023; Pohle & Thiel, 2020). A governance framework premised purely on boundary dissolution would misdescribe the present. The layered framework developed here is compatible with this reality because it does not require the erosion of state authority; it requires the recognition that state authority coexists with, and is mediated by, other sovereignty-like sites.

Near-term legal and practical steps

Several reforms are feasible in the short term. First, regulators can extend existing legal frameworks (data protection, consumer protection, competition law) to im-

mersive environments and can strengthen cross-border enforcement mechanisms; the GDPR's One-Stop-Shop model provides a template for coordinated oversight adaptable to biometric data and behavioural telemetry. Second, platforms should provide stronger transparency and auditability, with regulatory audits for algorithmic processes and biometric tracking treated as baseline obligations. Third, procedural fairness requires improvement: appeals processes, due-process safeguards, and clear explanations of sanctions can mitigate the legitimacy gap that currently characterises platform governance. These steps stabilise the system enough to enable deeper reforms.

Medium-term architectural commitments

More ambitious reforms require cooperation among states, platforms, and protocol communities. Interoperability is central. It can prevent monopolistic enclosure and enable cross-platform portability of identity, assets, and interactions, but it requires open standards rather than proprietary protocols. The European Commission's initiatives on open metaverse architectures suggest political will is emerging (European Commission, 2023). Privacy by design requires structurally minimising behavioural and biometric data rather than merely regulating *ex post*. Accountability infrastructure (protocol-level logging, audit trails, verifiable interactions) is needed to ensure remedial mechanisms have evidential grounding.

Research agenda

Much remains uncertain, and the research agenda set out here is intended to be elaborated rather than abbreviated. Four priorities stand out. First, sovereignty claims across layers require systematic mapping; the four-site account offered in Section 3 is a starting point, not a conclusion. Secondly, immersive harms require theorisation that is sensitive to the continuous, embodied, and spatial nature of metaverse interaction, and that can distinguish architectural from user-driven wrongdoing for remedial purposes. Thirdly, virtual property and avatar rights require renewed attention, because immersive environments complicate the distinctions between licences, ownership, and personhood that much private law presupposes. Fourthly, comparative research on Global South governance models is essential. It is essential for three specific reasons: much of the scholarly literature on digital sovereignty generalises from European and North American experiences, and cannot be assumed to travel (Chander & Sun, 2023; Couture & Toupin, 2019); states in the Global South confront digital sovereignty under conditions of infrastructural dependence and postcolonial legacy, giving rise to distinctive models of state, indigenous, and community authority (Jiang, 2024; Kukutai & Taylor, 2016);

and the metaverse, if it becomes genuinely global, will be shaped in material ways by regulatory choices made in regions where rule of law, capacity, and geopolitical positioning differ sharply from those in the Brussels-effect jurisdictions. Calibrated reforms, in short, demand interdisciplinary, comparative, and technically informed research. Integrating all four layers – legal, platform, protocol, and community – is how the metaverse becomes governable in a way that is both effective and principled.

References

Aguerre, C., Campbell-Verduyn, M., & Scholte, J. A. (2024). *Global digital data governance: Polycentric perspectives* (1st edn). Routledge. https://doi.org/10.4324/9781003388418

Arner, Douglas, Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. *Berkeley Technology Law Journal*, *37*(2), 623. https://doi.org/10.15779/Z38GF0MX5G

Beetham, D. (1991). *The legitimation of power*. Macmillan Education UK. https://doi.org/10.1007/978-1-349-21599-7

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world* (1st edn). Oxford University PressNew York. https://doi.org/10.1093/oso/9780190088583.001.0001

Bradford, A. (2023). *Digital empires: The global battle to regulate technology* (1st edn). Oxford University Press. https://doi.org/10.1093/oso/9780197649268.001.0001

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative Power Europe to the test of Iits geopolitical ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261–1280. https://doi.org/10.1111/jcms.13462

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

Castronova, E. (2005). *Synthetic worlds: The business and culture of online games*. University of Chicago Press.

Chander, A., & Sun, H. (Eds). (2023). *Data sovereignty: From the digital silk road to*

the return of the state (1st edn). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.001.0001

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press. https://doi.org/10.4159/9780674985933

Denardis, L. (2014). *The global war for internet governance*. Yale University Press. https://doi.org/10.2307/j.ctt5vkz4n

Douek, E. (2021). Governing online speech: From 'posts-as-trumps' to proportionality and probability. *Columbia Law Review*, *121*(3), 759–834.

Eder, N. (2024). Making systemic risk assessments work: How the DSA creates a virtuous loop to address the societal harms of content moderation. *German Law Journal*, *25*(7), 1197–1218. https://doi.org/10.1017/glj.2024.24

European Commission. (2023). *An EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition*. https://data.consilium.europa.eu/doc/document/ST-12092-2023-INIT/en/pdf

European Data Protection Board. (2018). *Guidelines 3/2018 on the territorial scope of the GDPR* (No. 3/2018). European Data Protection Board. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

European Data Protection Board. (2020). *Guidelines 04/2019 on Article 25 data protection by design and by default* (No. 04/2019). European Data Protection Board. https://edpb.europa.eu/system/files/2020-10/edpb_guidelines_201904_dataprotection_by_design_and_by_default_en.pdf

European Data Protection Board. (2021). *EDPB establishes cookie banner taskforce*. EDPB. https://www.edpb.europa.eu/news/news/2021/edpb-establishes-cookie-banner-taskforce_pl

European Data Protection Board. (2022a). *Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)* (No. 3/2022). European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-de-

cision-32022-dispute-submitted_en

European Data Protection Board. (2022b). *Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)* (No. 4/2022). European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-42022-dispute-submitted_en

European Data Protection Board. (2022c). *Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)* (No. 5/2022). European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-52022-dispute-submitted_en

European Data Protection Board. (2023a). *Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)* (No. 2/2023). European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en

European Data Protection Board. (2023b). *EDPB publishes urgent binding decision regarding Meta*. EDPB. https://www.edpb.europa.eu/news/news/2023/edpb-publishes-urgent-binding-decision-regarding-meta_en

European Data Protection Board. (2023c). *Report of the work undertaken by the Cookie Banner Taskforce*. European Data Protection Board. https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

European Data Protection Board. (2023d). *Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)* (No. 01/2023). European Data Protection Board. https://www.edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en

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 (General Data Protection Regulation)* (No. 2016/679). European Parliament and Council. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Parliament and Council. (2022). *Regulation (EU) 2022/1925 of the Euro-*

pean Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) (No. 2022/1925). European Parliament and Council. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

European Parliament and Council. (2026a). *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)* (No. 2022/2065). European Parliament and Council. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

European Parliament and Council. (2026b). *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)* (No. 2024/1689). European Parliament and Council. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Fairfield, J. (2005). Virtual property. *Boston University Law Review*, *85*, 1047.

Fairfield, J. (2022). Property as the law of virtual things. *Frontiers in Research Metrics and Analytics*, *7*, 981964. https://doi.org/10.3389/frma.2022.981964

Gentile, G., & Lynskey, O. (2022). Deficient by design? The transnational enforcement of the GDPR. *International and Comparative Law Quarterly*, *71*(4), 799–830. https://doi.org/10.1017/S0020589322000355

Gillespie, T. (2019). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press. https://doi.org/10.12987/9780300235029

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12), EU:C:2014:317.

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, *22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1), 205395171989794. https://doi.org/10.1177/2053951719897945

Habermas, J. (1996). *Between facts and norms: Contributions to a discourse theory of law and democracy*. MIT Press.

Hörnle, J. (2021). *Internet jurisdiction law and practice* (1st edn). Oxford University

Press. https://doi.org/10.1093/oso/9780198806929.001.0001

Husovec, Martin. (2023). Rising above liability: The Digital Services Act as a blueprint for the second generation of global internet rules. *Berkeley Technology Law Journal*, *38*(3), 884. https://doi.org/10.15779/Z38M902431

Huynh-The, T., Pham, Q.-V., Pham, X.-Q., Nguyen, T. T., Han, Z., & Kim, D.-S. (2023). Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence*, *117*(Part A), 105581. https://doi.org/10.1016/j.engappai.2022.105581

Jiang, M. (2024). Models of state digital sovereignty from the global south: Diverging experiences from China, India and South Africa. *Policy & Internet*, *16*(4), 727–738. https://doi.org/10.1002/poi3.427

Klonick, K. (2018). The new governors: The people, rules, and processes governing online speech. *Harvard Law Review*, *131*, 1598–1670.

Kukutai, T., & Taylor, J. (Eds). (2016). *Indigenous data sovereignty* (1st edn). ANU Press. https://doi.org/10.22459/CAEPR38.11.2016

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001

Lastowka, F. G., & Hunter, D. (2004). The laws of the virtual worlds. *California Law Review*, *92*(1), 1–73. https://doi.org/10.2307/3481444

Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. The MIT Press.

Lehdonvirta, V., & Castronova, E. (2014). *Virtual economies: Design and analysis*. MIT Press. https://doi.org/10.7551/mitpress/9525.001.0001

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.

Li, W., & Yang, D. (2024). Decentralized but coordinated: Probing polycentricity in EU data protection cross-border enforcement. In *Global digital data governance*. Routledge.

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

Moringiello, J. M. (2010). What virtual worlds can do for property law. *Florida Law Review*, *62*(1), 159.

Nissenbaum, H. (2005). Values in technical design. In C. Mitcham (Ed.), *Encyclopedia of science, technology, and ethics* (pp. 66–70). Macmillan.

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action* (1st edn). Cambridge University Press. https://doi.org/10.1017/CBO9780511807763

Ostrom, E. (2010). Polycentric systems for coping with collective action and global environmental change. *Global Environmental Change*, *20*(4), 550–557. https://doi.org/10.1016/j.gloenvcha.2010.07.004

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Porto, F. D., & Foà, D. (2023). *Defining virtual worlds: Main features and regulatory challenges – Issue paper*. https://cerre.eu/wp-content/uploads/2023/07/CERRE-Virtual-Worlds-Issue-Paper-0723.pdf

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2nd edn). Cambridge University Press. https://doi.org/10.1017/9781316822524

Shaw, M. N. (2021). *International law* (9th edn). Cambridge University Press. https://doi.org/10.1017/9781108774802

Shumin, C. (2022). *Jointly build a community with a shared future in cyberspace and create a brighter future in the digital era*. Chinese People's Institute of Foreign Affairs. https://www.cpifa.org/en/cms/book/365

Srnicek, N., & Sutter, L. (2016). *Platform capitalism*. Polity.

Suzor, N. P. (2019). *Lawless: The secret rules that govern our digital lives* (1st edn). Cambridge University Press. https://doi.org/10.1017/9781108666428

Taylor, T. L. (2006). *Play between worlds: Exploring online game culture*. MIT Press. https://doi.org/10.7551/mitpress/5418.001.0001

Tosoni, L. (2020). Article 60: Cooperation between the lead supervisory authority and the other supervisory authorities concerned. In C. Kuner, L. A. Bygrave, C.

Docksey, & L. Drechsler (Eds), *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 953–972). Oxford University Press. https://doi.org/10.1093/oso/9780198826491.003.0103

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, *25*(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

Xynogalas, V., & Leiser (Mark), M. R. (2024). The Metaverse: Searching for compliance with the General Data Protection Regulation. *International Data Privacy Law*, *14*(2), 89–105. https://doi.org/10.1093/idpl/ipae004

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