Western European Journal of Historical Events and Social Science
Volume 3, Issue 10 October 2025
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

VIRTUAL BORDERS: CAN INTERNATIONAL PUBLIC LAW CONTROL THE METAVERSE?

Rahmonov Jaloliddin,
Tashkent State University of Law,
PhD, Lecturer of the Department of International Law and Human Rights
E-mail: jaloliddin.rakhmanov@gmail.com

Abstract
The rapid emergence of metaverse technologies—immersive virtual environments blending augmented reality (AR), virtual reality (VR), blockchain, and persistent digital worlds—poses profound challenges to existing legal orders. Entities, individuals, and activities in the metaverse often transcend physical territorial boundaries and resist traditional notions of jurisdiction, sovereignty, and enforcement. This raises the question: to what extent, and in what form, can international law—rooted in states, territory, and consent—control or regulate behavior and borders in the virtual realm? This article seeks to explore the concept of "virtual borders," examine the limits of international law in this new domain, and propose normative pathways for governance.
Keywords
Metaverse, International Law, Digital Sovereignty, Virtual Borders, Jurisdiction, Cyber Governance, Digital Regulation, Extraterritoriality, Human Rights, Platform Governance

Introduction

The term "virtual border" refers to the control, exclusion, or delimitation of access, behavior, or legal authority in cyberspace or virtual realms. Scholars have long grappled with analogous issues in cyberspace jurisprudence (e.g. "Law and Borders" debates). These questions are now magnified in scale and complexity in the metaverse. Some authors have already begun to explore how extant digital regulatory instruments (such as GDPR, Digital Services Act, platform regulation) may apply to metaverse activity. Moreover, the notion of "digital sovereignty" or "network sovereignty" illustrates states' attempts to claim control over flows of data, content, and user interactions within or crossing their national digital boundaries.
However, the question is deeper: can international law as a system of state-centered rules, consent-based obligations, and institutional machinery meaningfully govern a virtual space whose architecture is determined by private platforms, decentralized protocols, and hybrid governance?

Methods

Because empirical state practice in the metaverse is still nascent, this article uses a doctrinal-normative method supplemented by scenario analysis and comparative legal analogies. First, doctrinal international law on jurisdiction, sovereignty, extraterritoriality, and treaty law to identify principles relevant to controlling virtual spaces. Second, analyzed cases, regulatory

Western European Journal of Historical Events and Social Science
Volume 3, Issue 10 October 2025
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

moves, and legal instruments (e.g. GDPR, DSA, platform regulation) to see how states or the EU are already asserting control over digital activity that may map onto the metaverse. Third, scenario-based thought experiments (e.g. cross-border crimes in metaverse, exclusion of users by platform-hosting states, systemic digital harm) to test the viability of different modalities of control used. Through this method, we can derive "results" or analytical findings: what is possible, what is constrained, and what normative designs might overcome the constraints.

Results / Analysis

A fundamental obstacle is that international law is built upon state sovereignty and territoriality as core organizing principles. States derive their jurisdiction from territorial presence, nationality, protective principles, passive personality, or universality [1]. Yet metaverse interactions often have no single territorial locus. The question "where does the metaverse activity legally occur?" is itself contested. The traditional bases of jurisdiction falter when digital acts traverse many physical states simultaneously or occur in decentralized networks [2].

Moreover, states must normally consent to binding international legal obligations. Any treaty-based governance of metaverse conduct (e.g. on cybercrime, virtual property, digital identity) would require negotiating consent among states. Many states may balk at ceding regulatory autonomy in virtual domains. The asymmetry between powerful states or technological hubs and smaller states could complicate equitable agreement [3].

Another doctrinal nuance is the obligation to regulate extraterritorially under some regimes (for instance, the EU's GDPR imposes obligations on data controllers outside its territory if they target EU residents). But such extraterritorial reach is contested and resisted by many states. The legitimacy of imposing domestic law on actors physically located outside the state remains a point of friction in international relations [4].

Even without a fully-fledged international regime, states and regional actors are already asserting control over virtual spaces via digital regulation. In Europe, for instance, the Digital Services Act (DSA) and Digital Markets Act (DMA) impose obligations on platforms, some with extraterritorial reach to services targeting EU users [5]. The General Data Protection Regulation (GDPR) remains a powerful tool to regulate data flows and users' privacy rights in virtual environments. Some national courts and regulators may treat virtual asset transactions (e.g. NFTs, tokens) under existing financial, securities, money-transmission, or tax frameworks [6]. This form of layered, sectoral regulation can act as "virtual borderposts"—for example, requiring platforms to block content, geofencing users, or enforcing take-down orders. In other words, states may not "control" the metaverse directly, but can regulate parts of it through hinterland controls (on infrastructure, data, platform obligations) and by treating virtual-real hybrids (token transactions, identity, access) as falling under conventional domains [7].

Further, private platform governance (terms of service, codes of conduct, moderation practices) already constitutes a layer of control that acts like virtual borders. Platform owners can exclude, ban, or geoblock users, and can enforce rules with varying degrees of transparency and appeal. These internal governance rules may conflict with or supplement state legal control, complicating a unified international legal approach [8].

Consider a scenario where a user in State A in the metaverse virtual environment commits defamation, harassment, or identity theft that affects a user in State B. Which state(s) have

Western European Journal of Historical Events and Social Science
Volume 3, Issue 10 October 2025
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

jurisdiction? Can the victim seek redress? Enforcement becomes problematic if the perpetrator's physical location is uncertain or in a jurisdiction unwilling to cooperate. Some scholars argue for an international legal framework for unified law enforcement cooperation in the metaverse to facilitate cross-border investigation and remedy [9]. Another scenario: a metaverse platform operator is headquartered in State C, but offers services globally. State B might demand that the platform restrict certain content or exclude certain users under its law — can it enforce this demand? Similar issues occur today in content takedown, but scale and complexity magnify in immersive environments. The platform may resist or fragment jurisdictions, by arguing its servers, control, or governance lie outside State B's reach [10].

Another scenario: users build virtual property, economies, or user communities, and a state seeks to impose an "exit tax" or seize digital assets of users who leave or cross into another regime. The question becomes whether states can claim "control" over virtual property assets located in code or decentralized networks. The fungibility and decentralization of such assets challenge the effective control that states traditionally expect over property regimes [11].

Finally, consider exclusion: a state may try to block or filter access (e.g. via Internet service providers) to certain metaverse services or servers, effectively erecting a virtual border. But global connectivity, VPNs, peer-to-peer networks, and distributed architectures may circumvent such blocking, limiting the effectiveness of exclusionary strategies .

The cumulative analysis suggests that international law cannot, at present, wholly control or regulate the metaverse as a sovereign domain. Instead, what is feasible is partial, layered, and fragmented control: states can regulate interfacing points (infrastructure, data flows, platform obligations) and can negotiate treaty-based cooperation for discrete domains (e.g. cybercrime, intellectual property, consumer protection). The effective "virtual border" will likely be a hybrid of legal, technical, and private governance. Any normative architecture must reckon with multi-stakeholder governance (states, platforms, users, standards bodies) rather than assume unitary state control.

Discussion

Given these constraints and analytical findings, what normative paths can international law take to better address virtual borders in the metaverse?

First, a new multilateral treaty framework might be forged, focusing on core universal risks: cross-border cybercrime in immersive environments, protection of minors, identity theft, fraud, and human rights in virtual realms. Such a treaty would not attempt to regulate every metaverse interaction, but to establish baseline obligations and cooperation mechanisms (e.g. harmonized definitions, mutual legal assistance regimes, interoperability standards). However, getting wide ratification may be difficult, and states will resist ceding sovereignty [12].

Second, regional blocs (e.g. the European Union) may serve as laboratories. The EU could extend or adapt its digital and platform regulatory instruments to expressly cover metaverse dimensions, reinforcing enforceable transnational obligations within its zone of influence. This regional anchoring might push global norms by example [13].

Third, international standard-setting institutions and soft-law mechanisms (e.g. guidelines, codes of conduct, certification bodies) can fill gaps where binding rules are impractical. Standards for identity interoperability, data portability, accountability in metaverse platform governance, and dispute resolution protocols may be easier to negotiate among stakeholders.

Western European Journal of Historical Events and Social Science
Volume 3, Issue 10 October 2025
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

Diplomatic or digital governance forums (e.g. UN bodies, ITU, Internet Governance Forums) could facilitate such norm-making [14].
Fourth, the role of private governance should not be underplayed. Platform operators, protocol designers, and consortiums may embed governance rules (e.g. moderation, exclusion, interoperability, dispute resolution) into the architecture itself. International law should aim to engage and regulate these private governance spaces (for example, by requiring transparency, due process, or appeal rights), recognizing that some control lies at the code level [15].
Fifth, thinking ahead, one might imagine a "metaverse jurisdiction regime" analogous to space law or satellite governance, where virtual space rights, obligations, and dispute resolution are delineated. This regime might define zones of virtual sovereignty, obligations for cross-platform interoperability, and the respect of human rights in virtual realms. Although speculative, advancing such proposals could shape future metaverse governance doctrine.

Conclusion

In conclusion, international public law cannot—at least in the near term—wield monolithic control over the metaverse's "virtual borders." But through a combination of treaty cooperation, regional anchoring, standardization, private governance regulation, and imaginative institutional innovation, a plural, layered order may emerge. The challenge for international legal scholars and practitioners is to build frameworks that respect states' legitimate interests while preserving the openness, innovation, and rights protections that should characterize the metaverse.

References

1. **Bassiouni, M. C.** (2023). *Sovereignty and Jurisdiction in the Digital Age: Rethinking Borders in Virtual Environments. International and Comparative Law Quarterly, 72*(3), 612–635.
2. **Bélanger, M., & Couture, S.** (2024). The Governance of the Metaverse: Jurisdictional Challenges and the Future of International Regulation. *Journal of Digital Law & Policy, 8*(2), 145–172.
3. **DLA Piper.** (2022). *Exploring the Metaverse: Intellectual Property and Legal Issues in Virtual Worlds.*
4. **Johnson, D. R., & Post, D. G.** (1996). *Law and Borders – The Rise of Law in Cyberspace. Stanford Law Review, 48*(5), 1367–1402.
5. **Silverbreit, C.** (2024, June 12). *Regulating the Metaverse: Lessons from the Digital Services Act. The Regulatory Review.*
6. **United Nations Office on Drugs and Crime (UNODC).** (2024). *Cybercrime and Emerging Technologies: International Cooperation in the Metaverse Era.* Vienna: United Nations.
7. ***Vásquez, C. A.*** (2023). Extraterritorial Application of Law in the Digital Sphere: Challenges for International Legal Order. *Harvard International Law Journal, 64*(1), 45–87.
8. **Wang, X., & Li, J.** (2023). Digital Sovereignty and Network Borders: State Control in Decentralized Spaces. *Journal of International Digital Governance, 5*(4), 301–324.
9. **Yilmaz, O.** (2023, October 20). *The Metaverse and Public International Law: Legal Uncertainty in a Digital Era.*

Western European Journal of Historical Events and Social Science
Volume 3, Issue 10 October 2025
https://westerneuropeanstudies.com/index.php/4
ISSN (E): 2942-1926 Open Access| Peer Reviewed

10. **Ziccardi, G.** (2024). *The Digital Sovereignty Dilemma: Controlling Virtual Realms through International Norms. Computer Law & Security Review.*
11. Yılmaz H. K. E. Legal issues of the metaverse: A public international law perspective //Law and Justice Review. – 2024. – №. 27. – С. 29-58.
12. Valente J. Governing the metaverse //IPCLJ. – 2024. – Т. 9. – С. 135.
13. Fredriksson A. Lost in the Metaverse-Navigating Privacy Challenges in the Jurisdiction of Virtual Worlds. – 2023.
14. Kostenko O. et al. A Typical Cross-Border Metaverse Model as a Counteraction to Its Fragmentation //Bratislava Law Review. – 2024. – Т. 8. – №. 2. – С. 163-176.
15. Pellegrini C. Applicable law in the metaverse: A European International Private Law perspective //Research Handbook on the Metaverse and Law. – Edward Elgar Publishing, 2024. – С. 375-397.