RESEARCH PAPER
Future Research in AI & IoT, 2025, 1(1)
Homepage: https://frai.journals.umz.ac.ir/
DOI:

International Law in the Metaverse Era: Towards a New Model of Regulatory

Zahra Mahmoudi Kordi *, Saeedeh Roomi[2]

[1] *Associate Professor, Department of Public and International Law, University of Mazandaran, Iran.*

[2] *Master's Degree in International Law, University of Mazandaran, Iran.*

Article Info
Received -----
Accepted -----
Available online -----

Keywords:
Metaverse; Web 3.0; Multilevel Governance; International Law; Human Rights; Digital Regulation; Rights-Based Regulation.

Abstract:
In this new age, cyberspace, in its course of evolution, has reached its third generation, namely the Semantic Web. In the world of Web 3.0, commonly referred to as the Metaverse, individuals interact with others through their digital identities, embodied in self-created avatars. The Metaverse, as an emerging ecosystem, has dissolved the traditional boundaries between the real and virtual worlds, introducing novel challenges to various concepts of international law, ranging from sovereignty and jurisdiction to international responsibility and human rights. Furthermore, the active participation of new actors, particularly technology-developing corporations alongside traditional actors, underscores the necessity of adopting a new regulatory approach. The present study, by critically examining various models of digital space regulation, aims to elaborate on the need to develop a new regulatory framework adapted to the specific features of this emerging ecosystem.

***Corresponding Author: z.mahmoudi@umz.ac.ir**

Supplementary information: Supplementary information for this article is available at https://frai.journals.umz.ac.ir/

Please cite this paper as:

1. Introduction

One of the defining characteristics of emerging technologies is their relentless and continuous advancement, to the extent that it may confidently be asserted that each moment witnesses the emergence of novel dimensions within the technology sector. Since the mid-twentieth century, when the rudimentary foundations of the Internet were first established, modern technologies have become an inseparable component of human existence. The Internet itself, as the fundamental platform for the development of the Web, has undergone profound transformations from its inception to the present day. The evolution of the Web is now categorized into three distinct generations: Web 1.0 ("read-only Web"), Web 2.0 ("social and collaborative Web")[1], and, most recently, Web 3.0 ("read, write, and execute Web"), a development largely attributed to the advent of decentralized technologies. To ascertain the precise meaning of this latest iteration of the Web, which serves as the foundational infrastructure for the emergence of the Metaverse, a forward-looking analytical perspective is essential. Web 3.0 constitutes a revolutionary development within the digital sphere, enabling users to actively participate in creating, managing, and utilizing data and information. This paradigm shift not only reshapes the modalities of user interaction but is also poised to redefine business models, the digital economy, and even the structures of social organization. Furthermore, Web 3.0—often referred to as the Semantic Web—utilizes artificial intelligence and machine learning technologies to function as a "global brain," processing content on both conceptual and contextual levels. Given that Web 3.0 provides the

[1] Concludes all of the features we currently associate with the Internet and social networks fall under this generation of the Web. It is an environment centered on interaction and participation, where users are not only able to read content but also contribute by writing and editing content on websites.

ISSN

underlying infrastructure for the development and administration of the Metaverse, its distinctive features reveal that the regulatory frameworks traditionally employed by the international community to govern cyberspace are insufficient for addressing the complexities of this new generation of the Web and the virtual world it engenders (i.e., the Metaverse). Notably, Web 3.0 is characterized by decentralization, whereby data and information are no longer subject solely to the control of centralized entities, such as major technology corporations.

Web 3.0 employs technologies such as blockchain, enabling users to exercise greater control over their personal data. One of its defining features is facilitating secure, decentralized transactions through blockchain-based infrastructures. Furthermore, as a user-centric model, Web 3.0 is grounded in decentralized identity systems, allowing individuals to establish and manage their identities independently, often anonymously.

The Metaverse is emerging as a virtual, multidimensional, and continuous environment where users actively engage, possess digital assets, and experience redefined economic systems, identities, and social interactions within a fully digital framework. As futurist Cathy Hackl has aptly stated, "The Metaverse is the convergence of our physical and digital lives. Through Web 3.0 technologies such as virtual reality, augmented reality, artificial intelligence, cloud computing, blockchain, and cryptocurrencies, we are able to connect with others via our digital identities."[2] Within this environment, individuals not only consume information and content but also generate revenue through their interactions.

Given the salient features of the Metaverse—such as decentralization, anonymity, transboundary nature, user-centered architecture, and endogenous digital economies—numerous legal challenges and, in some cases, significant threats to international law inevitably arise. These include, but are not limited to, challenges to state sovereignty and the erosion of governmental authority, as well as broader implications for various branches and subsystems of international law, including human rights law, intellectual property law, international criminal law, and the law of international responsibility.

These emerging threats and challenges underscore the urgent need to formulate innovative regulatory frameworks. This study, employing a descriptive-analytical methodology and grounded in library-based research, first examines the evolution of the Web—from its initial iterations to Web 3.0—and its role in enabling the development of the Metaverse. It then proceeds to address the fundamental question: what regulatory model is best suited to govern the Metaverse within the framework of international law? By analyzing various digital regulatory approaches—including self-regulation, state-based regulation, and hybrid models—the study ultimately proposes a normative framework based on rights-oriented polycentric governance. The findings suggest that a model rooted in rights-based polycentric regulation, integrating Elinor Ostrom's institutional theory of polycentric governance with the foundational principles of international human rights law, is not only capable of establishing an effective regulatory order for the Metaverse but also of ensuring its global and ethical legitimacy.

1.1. The Metaverse: A Novel Digital Ecosystem

The term Metaverse was first introduced in 1992 by science fiction author Neal Stephenson in his novel Snow Crash, wherein he depicted the Metaverse as a virtual utopia—a digital escape from the harsh realities of the physical world. [1] As an emerging concept undergoing continual evolution, defining the Metaverse remains a complex and unsettled task, with no universally accepted definition to date.

Etymologically, the term "Metaverse" is derived from two components: meta, meaning beyond, transcending, or transformation, and verse, meaning universe. In Persian, it is often translated as farajahan (literally "beyond-world" or "meta-world").

According to the Acceleration Studies Foundation (ASF), a nonprofit research organization in the field of emerging technologies, the Metaverse can be broadly categorized into three general types:

1. Virtual Worlds, where users immerse themselves in seamless fictional narratives;

2. Mirror Worlds, which replicate and reflect the existing physical world;

3. Augmented Reality (AR), which overlays real-world environments with digitally enhanced information using extended reality tools, capturing and storing data about individuals and objects in real time. [2]

Dirk Lueth, a serial entrepreneur, describes the Metaverse as "a parallel and immersive universe that merges with the physical world, where individuals appear through one or more distinct identities. Users are placed at the center of this universe, having full control over their personal data and digital assets. Enabled by blockchain technology, real ownership allows them to utilize, trade, and transfer assets within the Metaverse."[3] Similarly, Tommaso Di Bartolo defines the Metaverse as "the next generation of consumer interaction with technology—an immersive experience driven by a self-sustaining, community-centered economy that introduces a new digital reality, fostering shared value creation among users."[4]

Based on these perspectives, the Metaverse—particularly in its more advanced forms—rests on the infrastructure of

[2] https://medium.com/%40CathyHackl/making-money-in-the-metaverse-4efe59aebab8

[3] https://www.buildingtheopenmetaverse.org/episodes/digital-economies-in-the-metaverse

[4] https://skarredghost.com/2022/09/08/tommaso-di-bartolo-metaverse/?utm_source=chatgpt.com

Web 3.0. It is a digital, immersive, and interactive space built upon a convergence of emerging technologies, including augmented reality (AR)[5], virtual reality (VR)[6], extended reality (XR)[7], artificial intelligence, blockchain, and cryptocurrencies.[3] Within this environment, users engage through digital identities (avatars)[8], establishing social and economic interactions and engaging in creating, owning, and exchanging digital assets.

Given these dynamics, traditional state authorities and governance institutions do not hold the same position in the Metaverse as in conventional jurisdictions. Current evidence suggests that the primary actors in this space are, first and foremost, the technology companies developing the relevant infrastructure, followed by the users themselves. Within the Metaverse, individuals transcend national borders and cultural, linguistic, and even ideological differences, forming connections with others based on shared interests and personal affinities.

2. Regulatory Models of the Digital Space

The term regulation, in its specific legal sense, was first introduced in late 19th-century France to define the jurisdiction and functions of certain institutions responsible for overseeing and organizing private and autonomous activities in specific domains. Generally speaking, regulation refers to the deliberate and continuous action of public or private entities—based on predetermined standards—for shaping the conduct of regulated subjects, managing events or processes, or facilitating stakeholder engagement, all to ensure public welfare, interests, and the common good. The monitoring and enforcement of such regulation is undertaken either directly by the regulator or by involving relevant stakeholders. [4]

Digital regulation, as one of the most pivotal concerns in cyber governance, encompasses a set of norms, policies, institutions, and mechanisms aimed at guiding, overseeing, and organizing the activities, relationships, and consequences emerging from digital technologies and the virtual environment. It spans a broad spectrum of legal domains, including regulatory frameworks for artificial intelligence, blockchain technologies, and the Metaverse.

Digital regulation endeavors to strike a balance between innovation and open competition, digital rights and freedoms, the public interest, and national security. Since its emergence in the 1990s, the field of digital regulation has undergone significant evolution. In response to shifting technological landscapes, various regulatory models have been conceptualized and developed over time.

These models—understood as institutional and legal frameworks employed by states, international organizations, or regulatory bodies—serve to direct, control, and supervise digital spaces. In the 2020s, with the rapid and disruptive advances in areas such as artificial intelligence, the Metaverse, virtual and augmented realities, the Internet of Things, and blockchain, the need for forward-looking, flexible, and multi-layered regulatory approaches has become more urgent than ever.

2.1. The 1990s and the Predominance of the Self-Regulatory Model

Self-regulation refers to a form of governance whereby private actors—particularly corporations and industry stakeholders—establish their own behavioral rules, standards, policies, and enforcement mechanisms without direct governmental intervention. Certain legal scholars contend that, due to cyberspace's inherently integrated and transnational nature, traditional jurisdictional and legislative frameworks are ill-suited for regulating the internet and that a distinct regime of governance ought to be recognized for this domain. [7]

Under this model, specialized companies involved in internet-related activities are tasked with setting norms and imposing necessary restrictions to manage the virtual environment. The principal rationale for adopting self-regulation as a governance model for cyberspace lies in its decentralized and global characteristics. [8] Moreover, self-

[5] Augmented reality is a layer of digital artifacts projected spatially through devices such as smartphones, tablets, smart glasses, or contact lenses. It merges the physical environment with the virtual realm, enhancing the real world with digital details and complementing the user's perception of reality or their physical surroundings.

[6] Virtual reality is an entirely separate digital environment that serves as a substitute for the real world. Users in virtual reality experience a sense of immersion in an artificial space. It manipulates the senses to create the illusion of being in a different environment from the physical world. Through specialized equipment, users interact with the virtual space in ways similar to the physical world. Communication in virtual reality is enhanced by multisensory devices such as immersive helmets, VR headsets, and omnidirectional treadmills, enabling users to engage visually, auditorily, tactilely, and physically with virtual objects in a natural and responsive manner.

[7] Extended reality, also known as cross-reality, encompasses a range of immersive technologies and digital or electronic environments in which data is visualized. It includes virtual reality (VR), augmented reality (AR), and mixed reality (MR). Individuals interact with and perceive data within fully digital or semi-artificial environments created through advanced technologies. [5]

[8] In the third generation of the Web, individuals engage in interactions within a three-dimensional virtual world through avatars linked to their user accounts. The avatar serves as a representation of a person's presence in the metaverse. In this space, individuals are recognized as the controllers of their avatars, possessing authority over their appearance and behavior. Key concepts used to evaluate user experience within the metaverse include embodiment, sense of presence, and immersion. [6]

regulation is often regarded as a more straightforward and cost-effective alternative to traditional regulatory approaches. [9] Within this framework, ethical and practical responsibilities for oversight, control, and enforcement rest primarily with private industries and corporations.

In the 1990s, self-regulation emerged as a strategic response to concerns over state intervention in cyberspace. On the one hand, the internet during this decade represented a space of technological innovation; on the other, governments lacked experience in regulating digital environments, and their involvement was perceived as a potential impediment to innovation. The principles of self-regulation during this period were chiefly manifested through codes of conduct and ethical charters.

One of the most emblematic documents of this era is the 1996 Declaration of the Independence of Cyberspace by John Perry Barlow, which explicitly rejected the authority of nation-states over the digital realm. Another illustrative example is the early adoption of self-imposed regulatory frameworks by companies such as Netscape Communications and AOL. At a time when no comprehensive legal frameworks governed user conduct, these companies developed behavioral codes to manage content and user interactions. These codes laid the foundational principles that continue to shape content governance on today's social networks and digital platforms.

Examples of such early regulatory measures include fair use policies; prohibitions against the use of Netscape's services for unlawful activities (e.g., fraud, spam, or unauthorized access to other systems); emphasis on respectful and ethical online behavior; safeguarding user privacy and prohibiting the sharing of user data; privacy and security policies for online payments through the establishment of SSL encryption standards; user accountability for content; and bans on disruptive or network-compromising activities. [10]

2.2. 2000s: The Rise of State-Centric Regulatory Models

The 2000s marked a turning point in the cyberspace governance, witnessing the emergence of state-led regulatory initiatives. This shift was prompted by the proliferation of cybersecurity and terrorist threats, the rapid expansion of the digital economy and e-commerce, concerns over corporate transparency in data privacy practices, and the meteoric rise of digital platforms such as Facebook and Amazon.

State-centric regulation, as conceptualized by Barry Mitnick, refers to "the application of general administrative rules to private activities in accordance with prescriptive norms designed to serve the public interest." [11] In this model, regulatory authority is vested primarily in the state and its institutions, intervening through legal norms and public law instruments. [12]

Given the inherently transnational and extraterritorial nature of cyberspace, effective regulation cannot be achieved without interstate cooperation. As a result, implementing state-driven regulation involved enacting legislative frameworks, licensing regimes, censorship mechanisms[9], and supervisory controls at both national and international levels.

Consequently, this period saw the adoption of binding regulatory instruments in key digital domains at national and international levels. The regulatory frameworks were established to govern critical aspects of cyberspace, including data protection (e.g., the European Union's General Data Protection Regulation [GDPR], adopted in 2018[10]), electronic commerce[11], and cybercrime (e.g., the Budapest Convention, adopted in 2001 as the first international treaty on cybercrime).

Another hallmark of this era was the institutionalization of oversight, with the establishment and expansion of national and supranational regulatory bodies tasked with monitoring and enforcing digital governance.

2.3. The 2010s and the Emergence of a Hybrid Regulatory Model

The hybrid regulatory model, as the term implies, refers to a governance structure in which regulatory authority is not exclusively vested in the state or public institutions. Rather, it incorporates a range of actors—private entities, civil society organizations, corporations, and others—into the regulatory process. The essence of this model lies in the division of responsibilities between the state and the private sector. In effect, hybrid regulation represents a reconciliation between the paradigms of self-regulation and state-based regulation. [13]

[9] An example is China's Clean Internet Law, which includes filtering, content censorship, and control over online activities.

[10] The General Data Protection Regulation (GDPR) was enacted to safeguard the privacy and personal data security of European Union citizens. The regulation establishes stringent requirements for collecting, processing, storing, and transferring personal data. The GDPR adopts a broad and inclusive definition of "personal data," encompassing any information that can identify an individual either directly (such as a name or identification number) or indirectly (such as location data or online identifiers). Even data that appears anonymized may be classified as personal data if, when combined with other information, it can lead to the identification of a natural person.

[11] It is worth noting that although no comprehensive treaty has yet been concluded in this regard, the World Trade Organization (WTO) placed the issue of electronic commerce on its agenda in the late 1990s, and formal multilateral negotiations within the WTO framework have been underway since 2019. In addition to these efforts, certain regional agreements have also been concluded among states, one notable example being the Digital Economy Partnership Agreement (DEPA) between Singapore, New Zealand, and Chile.

From 2015 onwards, driven by the expansion of social media platforms and the emergence of crises related to the misuse of digital data, the need for regulatory mechanisms that were both flexible and technically sophisticated became increasingly evident. In response, the hybrid approach gained traction as a viable means of addressing the inefficiencies of self-regulation and the rigidity of state-centric models. Under this framework, while the government retains its legislative authority, private actors—including companies, platforms, civil society, and non-governmental organizations—are granted a participatory role in formulating and implementing regulatory norms.

More precisely, the state assumes responsibility for setting the foundational legal framework, whereas the development of technical standards and the operationalization of those norms is delegated to the private sector. This collaborative model offers distinct advantages, most notably the increased involvement of stakeholders and the emphasis on specialization and adaptability. Nevertheless, it is not without its challenges. Achieving coordination between public and private entities is inherently complex and may slow down the regulatory process. Moreover, if mechanisms for oversight and accountability are inadequately designed, there is a heightened risk that legal frameworks may be circumvented.

Above all, the potential for conflicts of interest looms large. Without effective state oversight, corporations may design regulatory standards that primarily serve their own interests. Consequently, the establishment of democratic control mechanisms—such as independent supervisory bodies—is essential to safeguard against regulatory capture and uphold compliance.

At the national level, the Australian Code of Practice on Disinformation and Misinformation has been cited as a successful example of the hybrid and participatory approach.[12] At the international level, two of the most comprehensive regulatory frameworks for online platforms—the European Union's Artificial Intelligence Act (2024) and the Digital Services Act (2022)—reflect a deliberate move away from the binary of rigid state regulation versus voluntary self-regulation.

- The European Union Artificial Intelligence Act

The EU Artificial Intelligence Act adopts a hybrid regulatory approach that integrates binding legal obligations—reflecting elements of state regulation—with voluntary standards and private sector participation, drawing from the logic of self-regulation. The core structure of the Act is built around a risk-based classification of AI systems, categorizing them into unacceptable, high, limited, or minimal risk levels. Using AI systems deemed to pose an "unacceptable risk" is strictly prohibited. High-risk systems—such as facial recognition in public spaces or AI used in recruitment and education—are subject to stringent requirements, including conformity assessments, compliance monitoring, and regular supervision. [14]

On the other hand, low-risk or minimal-risk systems are only subject to limited transparency obligations or, in some cases, are exempt from any legal mandate altogether. Alongside this strict regulatory architecture, the Act also encourages soft regulation. For instance, voluntary technical standards—such as ISO norms—are promoted to demonstrate compliance with legal obligations. Furthermore, the use of codes of conduct and trust labels has been envisioned to enhance transparency and accountability. [15] These mechanisms ensure a degree of regulatory flexibility while fostering the active involvement of private actors in the governance of AI systems.

Institutionally, the Act provides for the establishment of independent supervisory authorities, such as the AI Board[13], and seeks to foster cooperation among governments, technology firms, research institutions, and civil society. Thus, it exemplifies a genuinely collaborative and hybrid regulatory model.

- The Digital Services Act (DSA)

The Digital Services Act is one of the most significant legislative instruments for organizing the digital sphere and offers a novel model of hybrid regulation. It introduces a set of obligations concerning process transparency, reporting requirements, content moderation, and user rights. The Act seeks to respond to the growing power of digital platforms and the increasing complexity of online governance by blending binding legal norms with soft standards and self-regulatory mechanisms. [16]

In its binding regulatory dimension, the Digital Services Act (DSA) imposes a range of obligations on digital service intermediaries. These include reporting mechanisms, transparency requirements, effective procedures for removing illegal content, and cooperation with national authorities. The DSA introduces stricter obligations for large platforms, including risk assessments and annual independent audits. [17] These provisions reflect the state's role as a regulator and the implementation of stringent, binding legal norms.

Simultaneously, the DSA supports mechanisms of self-regulation and soft regulation, particularly in areas such as combating disinformation, the dissemination of political advertising, and the protection of children. Companies are encouraged to develop and apply voluntary codes of

[12] The Australian Government's Competition and Consumer Commission, in collaboration with digital platforms, has developed codes of conduct to protect consumer rights.

[13] The European AI Board is established under Article 56 of the draft European Union Artificial Intelligence Act. Operating within the framework of the European Commission, this body functions primarily as a coordinating mechanism among national supervisory authorities and serves as a provider of non-binding technical guidance in the implementation of the Act. The Board is composed of representatives from the Member States, alongside observers from various European institutions such as the European Commission, the European Union Agency for Fundamental Rights, and the European Data Protection Supervisor.

conduct and practice in these fields. [18] One example of a soft law instrument adopted under this framework is the "Code of Practice on Disinformation," which complements binding legal rules. [19]

Beyond its normative components, the DSA also establishes institutional mechanisms for shared oversight. The creation of the Digital Services Coordinators and the European Board for Digital Services illustrates the Act's orientation towards a hybrid governance model involving national, EU, and private-sector actors. Furthermore, by formalizing the role of intermediary bodies such as trusted flaggers, the DSA expands a system of shared responsibility.[14] These entities serve as the eyes and ears of civil society, assisting in the removal of illegal content—such as hate speech, violent materials, or copyright-infringing content—without relying solely on coercive state mechanisms. [20]

Overall, the DSA presents a compelling model for platform governance by integrating binding rules, voluntary standards, and innovative institutional structures—an approach that may serve as a blueprint for emerging regulatory domains, including the Metaverse.

3. In Search of an Appropriate Regulatory Model for the Metaverse

The emergence of the Metaverse as an immersive, participatory, and technology-driven virtual environment has generated foundational challenges in the realm of governance and regulation. Its decentralized architecture, the plurality of actors, technological complexity, and inherently transnational nature render traditional regulatory paradigms—whether state-centric or rooted in self-regulation—insufficient. As such, there is an urgent need to formulate a novel governance model tailored specifically to the Metaverse as an emergent digital domain. The key question then arises: Is the optimal framework merely a hybrid regulatory model, or must we seek a more distinct alternative?

Given that the hybrid regulatory approach has been proposed by various scholars and legal experts as a model for digital governance[15], this section first undertakes a critical examination of its applicability to the Metaverse. It assesses whether the hybrid framework—previously employed in regulating social media platforms at national and international levels—can adequately address the unique characteristics and legal demands of the Metaverse or whether an alternative regulatory model is required.

3.1. Can the Hybrid Model Meet the Metaverse?

It is readily apparent that owing to the global and borderless nature of the Metaverse—alongside its multiplicity of actors—purely state-based regulatory efforts confined to national jurisdictions are manifestly inadequate. Moreover, the technical specificity of underlying technologies such as NFTs, blockchain, and artificial intelligence necessitates the inclusion of private entities developing these technologies in regulatory rule-making processes. Thus, the hybrid model may offer several advantages for Metaverse governance, the most notable of which are outlined below:

Flexibility: The Metaverse is a dynamic and rapidly evolving environment. A regulatory framework that blends binding legal instruments with non-binding regulatory tools provides policymakers with the flexibility to adapt to swift technological developments.

Multi-Stakeholder Participation: Engaging diverse stakeholders—including private corporations, users, civil society organizations, and governments—can enhance both the legitimacy and effectiveness of regulatory outcomes.

Nonetheless, despite its widespread endorsement in the field of digital governance, the hybrid regulatory model encounters serious limitations in the international legal context, particularly when applied to the Metaverse. The distinctive attributes of the Metaverse, when contrasted with traditional interactive platforms (a distinction that mirrors the conceptual evolution from Web 2.0 to Web 3.0), introduce challenges that may render the hybrid approach inadequate on a global scale. The key limitations are analyzed as follows:

- Absence of a Global Central Regulatory Authority

The hybrid model presupposes the existence of a supervisory institution capable of mediating between public authorities and private entities. At present, no such institution with binding global jurisdiction exists. Unlike social media platforms, which operate within relatively centralized and bilateral systems, the Metaverse comprises a decentralized network of virtual spaces, many of which have ambiguous or anonymous ownership structures. Without a centralized oversight infrastructure, the global application of a hybrid regulatory model risks devolving

[14] According to Article 22 of the EU Digital Services Act, online platforms must establish mechanisms to receive reports from these credible reporters and provide an effective and prompt response.

[15] For more information on this, see:

- T. Alam (۲۰۲۴). Metaverse of Things (MoT) Applications for Revolutionizing Urban Living in Smart Cities, MDPI .

- Jingyi Wang (2025). Taxation of Crypto assets and Web 3.0: Web۳ Governance ،Routledge

- V. Mishchenko & S. Naumenkova (2025). Financial Metaverse Platforms, Financial & Credit Activity.

- Olney et al. (2024). Artificial Intelligence in Education and Metaverse: AI in Education (Springer).

into a tool of influence for dominant platforms rather than ensuring equitable governance. [21]

- Obstacles to International Coordination

Given the inherently transnational nature of the Metaverse, harmonizing national and regional regulatory frameworks within a hybrid structure poses a significant challenge. Divergences in legal traditions, regulatory priorities, and enforcement capacities may render coordination inefficient or ineffective.

- Conflicts of Interest Among Transnational Actors

As previously noted, under the hybrid model, technology corporations often assume a dual role as both norm-setters and subjects of regulation. In the Metaverse, where these corporations operate with profit maximization as a primary objective, their interests may directly conflict with global public welfare and core human rights norms. In practice, corporate self-regulation within the Metaverse may result in concentrated power and the circumvention of regulatory obligations. For example, Meta (formerly Facebook) simultaneously serves as both the developer and rulemaker within its own Metaverse platforms.

- Dominance of Major Technology Firms

Within hybrid regulatory structures, large technology corporations possess considerable bargaining power—often exceeding that of small or developing states.[22] Consequently, there is a real risk that hybrid governance may disproportionately reflect the interests of a few powerful American or Chinese companies rather than those of the international community as a whole.

- Weakness of Enforcement Mechanisms

In the event of regulatory non-compliance—such as violations of user privacy—what institutional mechanism would compel digital platforms to comply under a hybrid regime? As is well-established, the international legal system suffers from a persistent enforcement deficit, especially in relation to non-state actors operating across borders.

- Algorithmic Transparency and Independent Oversight

As previously discussed, algorithmic oversight constitutes a central feature of the hybrid model. However, in practice, ensuring global access to the underlying code and data for the purpose of neutral auditing remains infeasible. Without transparency, meaningful oversight is undermined. [23]

Overall, the metaverse, as a multidimensional, interactive, technological, and transnational construct, poses novel challenges to traditional models of regulation. State-centric regulation, which relies on territorial jurisdiction and unilateral sovereign authority, proves inadequate in addressing the extraterritorial nature of the metaverse. On the other hand, self-regulatory models—those driven by private sector initiatives—raise concerns regarding monopolistic dominance by major technology corporations and the potential erosion of users' rights and interests. Furthermore, treaty-based or international organization-centered regimes lack the necessary flexibility and responsiveness to effectively adapt to the rapid technological developments characterizing this domain. In light of these criticisms of the conventional regulatory triad, it must be acknowledged that although such approaches may remain functional at the national or regional level (such as within the European Union), they are ill-suited to govern a borderless and dynamic ecosystem such as the metaverse on a global scale. This raises a fundamental question: what regulatory model is best suited for the governance of the metaverse at the international level? The following section of this article will seek to address this inquiry.

3.2. Reimagining Polycentricity Governance through a Human Rights Lens

The metaverse, as a dynamic, technological, and inherently transnational environment, challenges the foundations of traditional governance and sovereignty. In such a context, regulatory frameworks must not only be grounded in multi-layered and multilevel institutional structures but also be fundamentally rooted in the human rights principles. Unlike conventional online platforms, the metaverse is not merely a space for information exchange; it constitutes an environment of presence, experience, agency, and even digital self-identification. In this space, the boundaries between the physical and virtual worlds blur; digital identities—or avatars—become equivalent to the legal personalities of users, and decisions or actions undertaken therein may have profound implications for freedom, security, dignity, and justice.

The rights-based regulatory theory, grounded in human rights as a universal and transnational normative system for protecting individuals' dignity, liberty, equality, and security against political and economic power, offers a normative, balanced, and human-centered framework for regulating the metaverse. When combined with the theory of polycentric governance, this model emphasizes the integration of institutional capacity with normative legitimacy—two essential elements for establishing a just order within the complex and global ecosystem of the metaverse.

The theory of polycentric governance, originally proposed by Elinor Ostrom, highlights the role of networked governance actors operating at multiple levels—national, regional, private, and civil society.[16] Within this framework, no single entity holds exclusive authority over rule-making and enforcement; rather, interaction among a plurality of institutions is paramount. According to Ostrom, a

[16] Elinor Ostrom has elaborated the theory of polycentric governance across several of her works; however, one of the most significant and coherent articulations of this theory appears in her seminal article titled "Polycentric Systems for Coping with Collective Action and Global Environmental Change," published in 2010 in the journal Global Environmental Change. This article stands as one of her key contributions to the field of commons governance, particularly at the global level and in the context of environmental challenges.

polycentric system comprises "a set of decision-making units with independent authority operating at multiple scales, which administer public matters through mutual interaction, competition, and cooperation". [24] This model emphasizes the coexistence of diverse institutions, the distribution of power, and structural flexibility. [25]

Given the metaverse's core characteristics, the polycentric model demonstrates high adaptability to this environment. The metaverse encompasses a wide array of actors—including states, platforms, decentralized associations, users, and tech companies—and therefore necessitates a governance model that can simultaneously acknowledge multiple centers of authority and facilitate cooperation among them. Moreover, the transboundary nature of the metaverse renders traditional, territorially bound governance structures inadequate. The horizontal and networked configuration of polycentric governance enables cross-border interactions among diverse stakeholders.

At the institutional level, the polycentric system permits the formulation of behavioral rules across various scales: micro-level (e.g., users or autonomous associations), meso-level (e.g., platforms), and macro-level (e.g., state and international institutions). This multi-tiered structure is reflected in Ostrom's Institutional Analysis and Development framework, commonly referred to as the "institutional ladder[17]", which identifies three primary levels:

1. Operational level: This level involves observable behaviors and decisions individuals make in their daily lives. For instance, in the metaverse, users make decisions about purchases, interactions, or content sharing. [26]

2. Institutional policy-making level (or rule-setting): This level involves decisions about creating, amending, or enforcing the rules at the first level. For example, platforms or user communities decide what content is permitted or which algorithms to use. This level is participatory and determines who has the right to make decisions at the operational level.

3. Legislative level: This is the most fundamental layer of governance and is concerned with the legitimacy of an institution. [27] The legislative level specifies who is authorized to create rules. Applying this model in metaverse governance clarifies which individuals are active at which levels and who has the right to set rules, which institution holds final decision-making authority, and whether there is a possibility of revisiting the fundamental rules and institutions.

At first glance, the polycentric governance model facilitates collaboration among actors and stakeholders at various levels within the metaverse, offering flexibility to address the complexities of this space while committing to self-regulatory mechanisms and accountability. This model prioritizes a network of institutions rather than focusing on a single law-making entity. By adopting this approach, international law moves beyond classical authoritarianism toward recognizing, coordinating, and enhancing the capacity of various institutions. However, as discussed further, polycentric governance is not a comprehensive solution. Therefore, this article proposes combining it with a rights-based approach.

The first reason for utilizing a rights-based approach is the lack of a coherent global normative framework within Ostrom's polycentric theory, which primarily focuses on institutional processes rather than the normative content of decisions. While the metaverse involves fundamental human rights issues such as privacy, algorithmic discrimination, freedom of expression, and human dignity, [28] the absence of a global normative framework like human rights makes it impossible to ensure justice and fairness in such governance.

The second reason is the failure to guarantee the rights of vulnerable groups. Polycentric governance is based on the principle of equality among actors and self-regulation, but in practice, vulnerable groups (such as children, minorities, or users in developing countries) may be excluded from decision-making processes. A rights-based approach can prevent such discrimination by establishing rights for stakeholders and responsibilities for those accountable. [29] Combining the polycentric theory with a rights-based approach ensures that companies are accountable to global norms like human dignity.

Another shortcoming of Ostrom's theory is its inability to address ethical and intercultural challenges, highlighting the need to integrate it with a rights-based approach. The metaverse, as a global ecosystem with diverse cultural and ethical backgrounds, requires basic ethical principles for peaceful coexistence. Ostrom's model is more suited to local issues and tangible resources (like forests or water resources) and does not address the ethical challenges of the digital space. A rights-based approach can play a complementary role in this area. [30]

Ensuring access to digital justice and effective remedy is a crucial issue that can only be achieved through adopting a rights-based approach, as the right to an effective remedy is one of the key principles of human rights in the digital space. [31] Mechanisms for judicial and non-judicial remedies (such as digital mediation or ethics commissions) must be established to effectively protect violated rights in the metaverse.

[17] The Institutional Ladder model, developed by Elinor Ostrom within the framework of polycentric governance analysis of common-pool resources, serves as a tool for understanding the various levels of institutional decision-making in addressing complex issues—particularly in contexts where centralized governance is ineffective, such as international arenas, shared resources, or virtual spaces. According to this theory, governance is not exercised in a unified or hierarchical manner but rather through multilayered and dynamic structures operating at different decision-making levels. These levels function like the rungs of a ladder, each playing a distinct role in the creation, modification, or implementation of rules.

As outlined above, the proposed combined model in this article emphasizes the simultaneous participation of governmental, international, private sector, and civil society institutions, provided that these actors adhere to global human rights principles. This framework respects both Ostrom's principle of diversity and rights-based principles of accountability and transparency. Consequently, it protects users' human dignity against algorithms and automated decisions, strengthens regulatory processes with accountability and effective participation, and creates tools for democratic oversight and operational transparency.

4. Conclusion

With the emergence of the metaverse as a new digital ecosystem, the traditional boundaries between the physical and virtual worlds have been dissolved. The transnational nature of the metaverse, its decentralized architecture, user anonymity, and endogenous economy have rendered classical governance models, including state regulation, self-regulation, and even hybrid models, ineffective within this space. A historical analysis of digital governance transformations reveals that while self-regulatory models, state regulation, and participatory frameworks each offer distinct advantages and limitations, the specific characteristics of the metaverse—such as the absence of central authority, challenges in international coordination, the risk of technological company dominance, and the necessity of safeguarding fundamental human rights—necessitate a rethinking of existing frameworks.

Effective governance of the metaverse requires the integration of technology with fundamental human and legal values. The future of the metaverse must be seen not only as a platform for technological innovation and interaction but also as a realm for the realization of freedom, dignity, and justice in the digital age. In this regard, the proposed model in this paper, i.e., human rights-centered polycentric governance, combines the principles of Ostrom's polycentric governance theory with normative frameworks of human rights, offering a flexible, participatory, and value-oriented approach to regulating the metaverse. This model facilitates the establishment of a network of governmental, private, and civil actors while relying on universal human rights principles to mitigate the threats posed by monopolistic power and technological abuse.

The human rights-centered polycentric model can ensure legitimacy and sustainability for the metaverse by establishing multilayered accountability mechanisms, promoting algorithmic transparency, strengthening meaningful stakeholder participation, and guaranteeing access to digital justice. However, effectively implementing this model requires overcoming challenges such as the lack of a global regulatory body, conflicts of interest among tech-driven actors, and the need for a human rights-based culture in the digital space. Consequently, the success of this model depends on the creation of independent international regulatory institutions and the definition of clear operational mechanisms for accountability and transparency. These issues may constitute the focus of future research in this field.

5. References

[1] Leenes, R. (2007). Privacy in the metaverse: Regulating a complex social construct in a virtual world. In IFIP International Summer School on the Future of Identity in the Information Society (pp. 95-112). Boston, MA: Springer US.

[2] Jeon, H. J., Youn, H. C., Ko, S. M., & Kim, T. H. (2022). Blockchain and AI Meet in the Metaverse. Advances in the Convergence of Blockchain and Artificial Intelligence, 73(10.5772), 73-82.

[3] Dozio, N., Marcolin, F., Scurati, G. W., Ulrich, L., Nonis, F., Vezzetti, E., ... & Ferrise, F. (2022). A design methodology for affective Virtual Reality. International Journal of Human-Computer Studies, 162, 102791.

[4] Hadavand, Mehdi; Jam, Farhad (2022). The concept of the regulatory state: analysis of regulation as a tool of governance, Strategic Quarterly Journal, Volume 30, Issue 2 - Serial Issue 99, pp. 266-227.

[5] Mystakidis, S. (2022). Metaverse. Encyclopedia, 2(1), 486-497.

[6] Davis, A., Murphy, J., Owens, D., Khazanchi, D., & Zigurs, I. (2009). Avatars, people, and virtual worlds: Foundations for research in metaverses. Journal of the Association for Information Systems, 10(2), 1.

[7] Cox, N. (2002). The regulation of cyberspace and the loss of national sovereignty. Information & Communications Technology Law, 11(3), 241-253.

[8] Netanel, N. W. (2000). Cyberspace self-governance: A skeptical view from liberal democratic theory. Calif. L. Rev., 88, 395.

[9] Land, M. (2013). Toward an international law of the internet. Harv. Int'l LJ, 54, 393.

[10] Reidenberg, J. R. (١٩٩٩). "Lex Informatica: The Formulation of Information Policy Rules Through Technology." Texas Law Review, ٧٦(٣), ٥٥٣.

[11] Christensen, Jørgen Grønnegård. (2011). Competing theories of regulatory governance: reconsidering public interest theory of regulation. In David Levi-Faur (Ed.), Handbook on the Politics of Regulation (pp. 96-110). Massachusetts: Edward Elgar Publishing.

[12] Black, Julia. (2002). Critical Reflections on Regulation. Australian Journal of Legal Philosophy, 1(27), 1-35.

[13] Schulz, W., & Ollig, C. (2023). Hybrid Speech Governance: New Approaches to Govern Social Media Platforms under the European Digital Services Act?. J. Intell. Prop. Info. Tech. & Elec. Com. L., 14, 560.

[14] Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International, 22(4), 97-112.

[15] Hacker, P. (2023). AI regulation in Europe: from the AI act to future regulatory challenges. arXiv preprint arXiv:2310.04072.

[16] European Commission. (2022). 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).

[17] Husovec, M. (۲۰۲۳). The EU's Digital Services Act and Platform Regulation: Between Fundamental Rights and Regulatory Innovation. Yale Law School Working Paper.

[18] De Streel, A., Bourreau, M., Feasey, R., Fletcher, A., Kraemer, J., & Monti, G. (2024). Implementing the DMA: substantive and procedural principles. Centre on Regulation in Europe (CERRE) asbl.

[19] Helberger, N. (۲۰۲۳). Platform power, democracy and the DSA: How the Digital Services Act tries to reboot platform governance in Europe. Internet Policy Review, ۱۲(۱), ۱–۱۸.

[20] Douek, E. (2022). The siren call of content moderation formalism. NEW TECHNOLOGIES OF COMMUNICATION AND THE FIRST AMENDMENT: THE INTERNET, SOCIAL MEDIA AND CENSORSHIP (Lee Bollinger & Geoffrey Stone eds., 2022 Forthcoming).

[21] Belli, L., & Venturini, J. (2016). Private ordering and the rise of terms of service as cyber-regulation. Internet Policy Review, 5(4), 1-17.

[22] Zuboff, S. (2023). The age of surveillance capitalism. In Social theory re-wired (pp. 203-213). Routledge

[23] Morozov, E. (2014). To save everything, click here: the folly of technological solutionism. J. Inf. Policy, 4(2014), 173-175.

[24] Ostrom, E. (2010). Beyond markets and states: polycentric governance of complex economic systems. American economic review, 100(3), 641-672.

[25] Aligica, P. D., & Tarko, V. (2012). Polycentricity: from Polanyi to Ostrom, and beyond. Governance, 25(2), 237-262.

[26] Ostrom, E. (2009). Understanding institutional diversity. Princeton university press.

[27] McGinnis, M. D., & Ostrom, E. (2014). Social-ecological system framework: initial changes and continuing challenges. Ecology and society, 19(2).

[28] Cuellar, D. P., Lasso, A. V., & Salazar, A. B. (2024). The metaverse: an analysis from a human rights perspective. Revista Jurídica Mario Alario D´ Filippo, 16(33), 202-218.

[29] United Nations Office of the High Commissioner for Human Rights (۲۰۲۰). The Right to Privacy in the Digital Age.

[30] Stahl, B. C., Schroeder, D., & Rodrigues, R. (2023). Ethics of artificial intelligence: Case studies and options for addressing ethical challenges (p. 116). Springer Nature.

[31] United Nations Office of the High Commissioner for Human Rights (۲۰۲۲). Access to Remedy in the Digital Age.