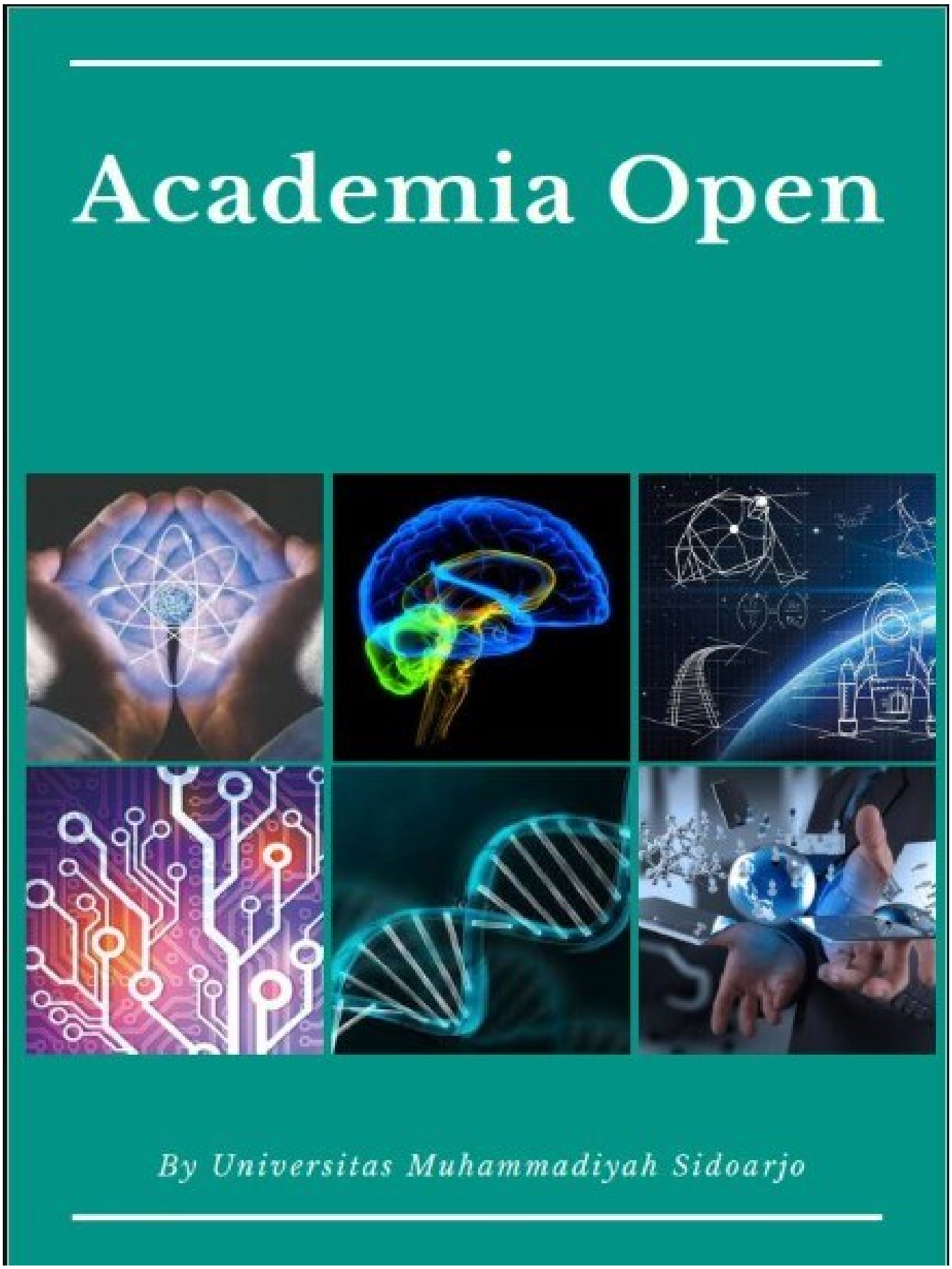
Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764



ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

Table Of Contents

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

EDITORIAL TEAM

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

Adaptive Metaverse Regulation for Digital Legal Anomie in Indonesia

Nanang Febriyanto, nanangfeb121@student.uns.ac.id (*)
Faculty of Law, Sebelas Maret University, Surakarta, Central Java, Indonesia

Sapto Hermawan , saptohermawan_fh@staff.uns.ac.id
Faculty of Law, Sebelas Maret University, Surakarta, Central Java, Indonesia

Hari Purwadi, hpurwadie@staff.uns.ac.id
Faculty of Law, Sebelas Maret University, Surakarta, Central Java, Indonesia

(*) Corresponding author

Abstract

General Background The rapid emergence of the Metaverse, characterized by immersive virtual spaces integrating blockchain and artificial intelligence, has fundamentally transformed social, economic, and cultural interactions. **Specific Background** Despite the socioeconomic opportunities offered by these virtual environments, their development has outpaced the existing legal system, leaving a void in regulatory guidance. **Knowledge Gap** While current research largely concentrates on technical aspects or data protection, there remains a critical need to analyze the resulting legal anomie and evaluate international regulatory models to formulate a comprehensive national policy framework. **Aims** This study investigates the legal anomie within the Metaverse ecosystem, examines regulatory approaches across international jurisdictions, and proposes an adaptive legal paradigm for Indonesia. **Results** The findings reveal that current legal norms fail to address issues such as avatar-based harassment, digital identity theft, and cross-border jurisdiction, leading to a state of normative uncertainty. Comparative analysis shows that diverse models, ranging from rights-based approaches to industry self-governance, exist globally. **Novelty** The study synthesizes these findings into a unique adaptive legal paradigm underpinned by four core principles: technology neutrality, human-centric governance, platform accountability, and cross-border cooperation. **Implications** This paradigm offers a responsive foundation for developing Indonesian Metaverse governance that balances technological innovation with the robust protection of user rights, providing a path toward legal certainty in virtual spaces.

Highlights:

- Rapid Metaverse growth has created a condition of legal anomie characterized by significant regulatory gaps in digital identity and biometric protection.
- Traditional territorial jurisdiction concepts are rendered inadequate by the cross-border and decentralized nature of immersive virtual environments.
- An adaptive legal paradigm based on platform accountability and human-centric governance is essential for balanced digital innovation and rights protection.

Keywords: Digital Regulation, Legal Anomie, Metaverse, Platform Accountability, Virtual Space Governance

Published date: 2026-06-30

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

Introduction

Global digital transformation has entered a new phase marked by the emergence of the Metaverse , an immersive virtual space that allows individuals to interact, work, transact, and build social identities in a three-dimensional digital environment. Unlike previous generations of the internet, which focused on exchanging information through two-dimensional media, the Metaverse offers a virtual presence experience *that creates* a sense of direct involvement in a digital environment. This technological development is projected to become the foundation for the next generation of the digital economy because it integrates various technologies such as *Virtual Reality* (VR), *Augmented Reality (AR), and Artificial Intelligence (AI). Reality* (AR), *Artificial Intelligence* (AI), *blockchain* , and *the Internet of Things* (IoT) [1].

The emergence of the Metaverse has transformed the way humans understand the concepts of space, identity, and social interaction. Activities that previously could only be done physically can now be replicated in virtual environments with increasing levels of immersion . The world of education is starting to utilize virtual spaces for interactive learning simulations, the business sector is developing digital asset-based trading models, while global companies are starting to adopt virtual workspaces as an alternative for professional interaction [2]. These developments demonstrate that the Metaverse is not just a technological innovation, but a social transformation that has the potential to change the structure of human relationships in various aspects of life.

Despite offering various opportunities, the development of the Metaverse has also given rise to increasingly complex legal issues. Various forms of violations previously known in physical spaces are starting to emerge in new forms in virtual environments, such as sexual harassment through avatars , digital identity theft, virtual asset fraud, intellectual property rights violations, and the misuse of user biometric data [3]. These issues demonstrate that technological developments are moving much faster than the ability of the law to regulate human behavior in the digital space. As a result, a condition has emerged that can be categorized as legal anomie , namely a situation where existing norms are no longer able to provide adequate guidance for society in dealing with rapid social change [4].

The concept of anomie proposed by Émile Durkheim is relevant in explaining this phenomenon. Durkheim argued that rapid social change can cause an imbalance between societal development and the ability of normative systems to regulate individual behavior [5]. In the context of the Metaverse , this imbalance is evident in the absence of clear legal standards regarding the legal status of avatars , digital identity protection, virtual platform liability, or dispute resolution mechanisms that occur in virtual environments. As a result, various actions that substantially harm individuals often fall within a *legal gray area* .

This issue is further complicated because the Metaverse operates in a digital environment that is cross-border (*borderless) .environment*). This characteristic poses a serious challenge to the concept of jurisdiction that has been the basis of modern law enforcement. An action carried out by a user in one country can impact victims in another country through a platform whose servers are located in a different jurisdiction. This condition raises fundamental questions about which country's law applies, which court has the authority to try, and how law enforcement mechanisms can be carried out effectively in a virtual space that knows no geographical boundaries [6].

Various countries have begun to respond to these challenges through varying regulatory approaches. The European Union has developed a strict regulatory-based approach through *the Digital Services Act* (DSA) and *the Artificial Intelligence Act (AI) . Intelligence An Act* that emphasizes platform accountability and user protection [7]. The UK has chosen a more flexible approach by optimizing existing legal instruments through *the Online Safety Act. Act* and data protection regulations [8]. On the other hand, South Korea developed a collaborative governance model through the Korean The Metaverse Alliance involves government, industry, and academia in formulating ethical standards and governance for the Metaverse [9]. Meanwhile, Japan places even greater emphasis on a *self-governance approach* by providing industry players with ample space to develop internal regulatory mechanisms [10].

These differing approaches demonstrate that, to date, there is no single regulatory model that can be considered a universal solution for governing the Metaverse . On the one hand, overly stringent regulations have the potential to hinder technological innovation and digital investment. On the other hand, an overly lax approach can result in weak protection of user rights. This situation highlights the need to formulate a new legal paradigm that maintains a balance between human rights protection, legal certainty, and the development of technological innovation.

Previous research has generally focused on the technical aspects of the Metaverse , personal data protection, or the digital economic opportunities it creates. However, there is still relatively limited research specifically linking the phenomenon of legal anomie in the Metaverse with a comparative analysis of various international regulatory models as a basis for formulating national legal policies. Yet, a comparative approach is crucial for identifying best practices *.practices*) while avoiding regulatory failures that have been experienced by other countries.

Based on the above-mentioned context, this study aims to analyze the forms of legal anomie that emerge in the Metaverse ecosystem , examine various regulatory approaches applied in several international jurisdictions, and formulate an adaptive legal paradigm that can serve as a foundation for developing Metaverse regulations in Indonesia. This study offers a novelty in the form of a synthesis of regulatory models based on four main principles: *technology ,neutrality , human-centric governance , platform accountability* ,and *cross -border cooperation as a foundation for* Metaverse governance that is responsive to technological developments while ensuring the protection of user rights.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

Method

This research is normative legal research *that focuses on* the study of legal norms, legal principles, doctrines, and policies related to Metaverse governance from a national and international legal perspective. The normative approach was chosen because the main problem studied does not lie in the empirical behavior of society, but rather in the gap between the development of Metaverse technology and the ability of the legal system to provide certainty, protection, and justice for users of virtual spaces [11].

This research uses three main approaches, namely *statutory approach* , *comparative approach* ,and *conceptual approach*. *Statutory* regulatory approach*approach*) is used to identify and analyze various legal instruments relevant to digital space governance, both national and international. The instruments analyzed include the European Union's *Digital Services Act (DSA), Artificial Intelligence Act (AI*), and the European Union's Digital Services Act (DSA). *Intelligence Act* (AI Act), *Online Safety English Act , South Korea's* Metaverse ethical guidelines , as well as various international human rights instruments such as *the Convention on the Elimination of All Forms of Discrimination Against Women (* CEDAW) and *International Covenant on Civil and Political Rights* (ICCPR) [12].

Comparative approach*approach*) is used to evaluate the regulatory models implemented by various countries in response to the development of the Metaverse . This approach is based on the assumption that legal issues arising from digital technology are global in nature, so that the experiences of other countries can be an important source of learning in formulating national legal policies [13]. Through this approach, the study not only compares the content of regulations but also analyzes the regulatory philosophy, the pattern of relations between the state and industry players, the level of user protection, and the effectiveness of law enforcement mechanisms developed by each jurisdiction.

Meanwhile, the conceptual approach (*conceptualThe metaverse approach* is used to construct a theoretical framework for this research through an analysis of various concepts related to legal anomie, digital governance, responsive law, and human rights protection in virtual environments. This approach is important considering that the development of the Metaverse presents various new phenomena that cannot yet be fully explained through conventional legal categories. Therefore, this research not only examines existing legal norms but also seeks to develop legal constructions capable of addressing future challenges [14].

The legal materials used in this research consist of primary, secondary, and tertiary legal materials. Primary legal materials include international regulations, human rights instruments, and official policies related to digital governance. Secondary legal materials consist of books, scientific journal articles, research reports, and academic publications discussing the Metaverse , cyber law, digital jurisdiction, technology ethics, and contemporary legal theory. Tertiary legal materials are used as supporting materials to explain technical terms and concepts developing within the digital ecosystem.

Data analysis was conducted qualitatively through two main stages. The first stage used *content analysis. analysis* to identify regulatory patterns developing in various international legal instruments and national policies that are the object of research. This analysis aims to find general trends regarding how countries respond to legal issues that arise in virtual space [15]. The second stage is carried out through comparative legal analysis to compare the strengths, weaknesses, and implications of each regulatory model implemented by the European Union, the United Kingdom, South Korea, and Japan. This comparative analysis is not only oriented towards identifying regulatory differences, but also directed at finding legal principles that have the potential to be adopted in the Indonesian context.

In contrast to legal research, which is merely descriptive, this study uses a prescriptive approach to generate policy recommendations. The prescriptive approach was chosen because the primary objective of the research is not simply to explain the prevailing legal conditions (*iusconstitutum*), but rather formulates the direction of legal development that should be formed (*iusconstituendum*) to face the challenges posed by the Metaverse [16]. Through a process of synthesis of the results of the analysis of international regulations and the legal theories used, this study develops an adaptive legal paradigm consisting of four main principles, namely *technology neutrality , human- centric governance , platform accountability* , and *Cross -border cooperation . These four principles then serve as the basis for formulating policy recommendations for Indonesia to develop* Metaverse governance that is responsive to technological developments while ensuring the protection of user rights.

Through a combination of normative, comparative, and conceptual approaches, this research is expected to produce an analysis that not only explains the phenomenon of legal vacuum in the Metaverse , but also provides theoretical and practical contributions to the development of digital regulation in Indonesia.

Results and Discussion

A. Legal Anomie in the Metaverse Ecosystem

The development of the Metaverse has given rise to a new social space that is no longer entirely subject to the physical or territorial boundaries of a country. Unlike previous generations of social media that functioned as a means of communication and information exchange, the Metaverse presents a digital environment that allows users to build identities, engage in economic activities, form social relationships, and even experience interactions that resemble real life through avatar representation . This transformation shows that the Metaverse is not simply an evolution of digital technology, but has developed into a social ecosystem with its own structure, norms, and dynamics [17].

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Amidst these developments, the law faces a fundamental challenge in the form of the inability of existing norms to keep pace with the pace of technological innovation. This condition can be understood through the concept of anomie introduced by Émile Durkheim defines anomie as a situation where social change occurs more rapidly than the ability of social institutions to provide clear behavioral guidelines for society [18]. In the context of the Metaverse , anomie arises when various digital activities that have social, economic, and psychological consequences have not received adequate legal regulation, thus creating a space for normative uncertainty .*uncertainty*).

The phenomenon of anomie in *the* Metaverse is evident in the increasing number of forms of violation that are difficult to qualify using conventional legal categories. One example that has received the most attention is sexual harassment through avatars (*harassment*). The case of Nina Jane Patel on Meta's Horizon Worlds platform in 2021 serves as an important illustration of how actions occurring in virtual spaces can have a real psychological impact on victims [19]. Although there was no physical contact as in the traditional sense of sexual violence, the experience still resulted in feelings of fear, loss of safety, and psychological trauma that substantially share characteristics with real-world violence.

This phenomenon demonstrates that the legal paradigm, which has historically relied on the dichotomy between the physical and digital worlds, is beginning to lose its relevance. From a classical legal perspective, legal losses are generally measured based on physical damage, loss of property, or violation of concretely identifiable rights. However, the Metaverse presents a new, more complex form of loss, as it relates to a person's digital identity, psychological integrity, and virtual existence. As a result, various actions considered socially detrimental often cannot be effectively addressed by available legal instruments [20].

This condition is further strengthened by the development of *virtual reality* (VR) and *extended reality technology*. *Virtual reality* (XR) creates immersive experiences with a high level of emotional engagement. Research shows that the human brain often responds to virtual experiences in ways not significantly different from physical experiences, especially when individuals feel a *sense of presence*. *of presence*) in the digital environment [21]. Therefore, the view that considers actions in the Metaverse as merely a “virtual game” is becoming increasingly difficult to maintain, considering that the impact it has can go beyond the boundaries of digital space and affect the psychological state of users in real terms.

avatar harassment , legal anomie in the Metaverse is also reflected in the increasing risk of digital identity abuse. In virtual ecosystems, user identity not only serves as an authentication tool , but also represents a person's social and economic existence. Avatars can have reputations, digital assets, social networks, and even high economic value. Thus, digital identity theft or manipulation can no longer be viewed as merely an administrative violation, but has the potential to cause losses equivalent to identity theft in the real world [22].

Another issue that demonstrates a lack of norms is the management of user biometric data . Unlike conventional digital platforms, the Metaverse relies on the collection of far more sensitive data, such as body movement patterns, facial expressions, eye gaze, emotional responses, and even voice characteristics. This data allows platforms to build highly detailed behavioral profiles that can potentially be used for commercial purposes or psychological manipulation [23]. In such circumstances, personal data protection is no longer solely concerned with identity information, but also concerns an individual's cognitive and emotional aspects, which are part of the most fundamental right to privacy.

From a legal theory perspective, this situation indicates that the root of the Metaverse problem is not simply the lack of specific regulations, but rather the legal paradigm's lag in responding to the changing social structures shaped by digital technology. Most modern legal systems are built on the assumption that human activity takes place within a physical space that can be identified territorially. As a result, concepts such as jurisdiction, locus of crime , proof, and legal responsibility are designed to deal with social realities that differ from the characteristics of today's virtual space [24].

This view is in line with Lawrence Lessig's thinking , which states that in cyberspace, human behavior is not only regulated by state law (*law*), but also by technological architecture (*code*), social norms (*norms*), and market mechanisms (*market*) [25]. In the context of the Metaverse , the program code designed by the platform often has a greater influence than state regulations in determining user behavior. Security features, moderation systems , privacy settings, and reporting mechanisms built by the platform in practice become the main regulatory instruments that govern the daily lives of users.

This situation creates a digital governance paradox. On the one hand, the state has a constitutional obligation to protect citizens' rights from various forms of violation. However, on the other hand, most of the virtual spaces where these violations occur are under the control of global technology corporations operating across jurisdictions. As a result, regulatory functions have shifted from the state to digital platforms, which in many cases lack adequate accountability mechanisms. [26]

From the perspective of *Responsive Law* developed by Nonet and Selznick , this anomie demands a shift in perspective on the function of law. Law can no longer be positioned as an instrument that merely reacts after a violation occurs, but must evolve into a system capable of anticipating the social impacts of technological developments [27]. Therefore, regulating the Metaverse requires a more adaptive, multidisciplinary approach, oriented toward protecting humans as the center of technological development.

Based on this, legal anomie in the Metaverse cannot be understood simply as a regulatory vacuum. This phenomenon reflects the tension between the acceleration of technological innovation and the legal system's ability to maintain its fundamental function as an instrument for protecting rights, creating legal certainty, and maintaining social order. If this condition is not addressed promptly through the development of an adaptive legal paradigm, the development of the

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14764

Metaverse has the potential to create a new social space that will evolve faster than the state's ability to regulate it.

B. Metaverse Regulatory Models Across Jurisdictions

The development of the Metaverse has prompted various countries to formulate different regulatory strategies according to the characteristics of their respective legal systems, levels of technological development, and public policy orientations. To date, there is no international legal instrument that specifically regulates the Metaverse comprehensively. As a result, countries have developed diverse regulatory approaches, ranging from *hard models to... law* that emphasizes strong state intervention to a *soft approach Laws* that provide greater space for industry to self-regulate. These differences indicate that Metaverse governance is still in the regulatory stage *.experimentation*), so comparative studies are important to identify best practices that can be used as a reference for Indonesia.

The European Union is one of the most progressive jurisdictions in developing a regulatory framework for the digital space. The EU's approach is based on the view that technological development must always be within the framework of protecting citizens' fundamental rights. This principle is reflected in *the Digital Services Act* (DSA), which positions digital platforms as actors legally responsible for the risks arising from the operation of their systems [28]. In the context of the Metaverse , this approach has important implications because platform providers are no longer viewed as passive intermediaries. intermediary), but rather as an entity that has an obligation to prevent, detect, and handle various forms of violations that occur in the virtual environment.

Besides DSA, the European Union is also developing *Artificial Intelligence Act* that regulates the use of artificial intelligence systems based on the level of risk posed to user rights [29]. Some of the technologies that form the foundation of the Metaverse , such as *biometric categorization , emotion recognition* and *behavioral Profiling* , categorized as a high-risk *AI system* ,must meet strict standards of transparency, accountability, and oversight before it can be widely used. This approach demonstrates the EU's adoption of a *rights-based paradigm*. *regulation* , namely a regulatory model that places the protection of human rights as the main objective of regulating digital technology.

Despite providing a high level of protection, the European Union's approach has also faced criticism. The complexity of the legal obligations imposed on platform operators has the potential to increase compliance costs *.cost*) and inhibit innovation, especially for start-up companies that have limited resources [30]. From a digital economy perspective, overly strict regulations can create barriers to entry (barriers) . to entry) which ultimately strengthens the dominance of large technology companies that have the capacity to meet these regulatory requirements. Therefore, the European Union model is often seen as successful in terms of user protection, but it still faces challenges in maintaining the balance between regulation and innovation.

In contrast to the European Union, the UK has developed a more pragmatic and evolutionary approach. The UK government has not enacted specific legislation regarding the Metaverse , but rather has optimized existing legal instruments to address the various issues that arise in virtual spaces. This approach is based on the assumption that technological development is occurring too rapidly, and the creation of overly specific regulations risks becoming obsolete quickly [31]. Therefore, the UK has chosen to utilize various existing instruments, such as *Online Safety Act* , UK *General Data Protection Regulation* (UK GDPR), as well as the intellectual property law regime to regulate activities within the Metaverse .

The advantage of the UK approach lies in its flexibility. By leveraging existing legal frameworks, the government can respond to technological developments without having to wait for a lengthy legislative process. However, this approach also raises the issue of regulatory fragmentation. Because different aspects of the Metaverse are governed by different legal instruments, it often presents difficulties in determining an integrated legal protection mechanism [32]. In practice, users must contend with multiple legal regimes with differing objectives and enforcement mechanisms, potentially creating legal uncertainty.

Meanwhile, South Korea opted for a more collaborative governance model through the formation of *the Korean Metaverse Alliance* (KMA). This approach reflects a *co-regulation strategy* , namely regulation carried out through collaboration between government, industry, academia, and other stakeholders [33]. Through this forum, the government functions not only as a regulator, but also as a facilitator that encourages the growth of the national Metaverse ecosystem .

The South Korean model is appealing because it seeks to strike a balance between innovation and user protection. The government recognizes that overly stringent regulations can hinder the development of the growing digital industry. Therefore, various ethical guidelines and standards of conduct were developed through a consultative mechanism that directly involves industry players. This approach provides high flexibility because standards can be updated quickly to reflect technological developments. However, its main weakness lies in the low enforceability of the law, as most of the instruments used are *soft*. *law* , its effectiveness depends heavily on the level of voluntary compliance from industry players [34].

In contrast to South Korea, Japan has adopted an approach that places greater emphasis on *self-governance* . The Japanese government provides technology companies with ample space to develop internal regulatory mechanisms based on the characteristics of each platform [35]. This approach is based on the belief that industry players have a better understanding of the technology they develop than state regulators. For this reason, the state plays a more facilitative role, providing general guidelines without over-intervening. The Japanese approach has the advantage of fostering a climate of innovation and encouraging creativity in the digital industry. However, from a user protection perspective, this model faces significant risks. Different protection standards across platforms can create disparities in handling legal violations. Furthermore,

companies' commercial interests do not always align with user protection interests. In certain situations, companies may prioritize user growth and economic profit over enforcing strict ethical standards [36].

Identifying legal disparities among the four jurisdictions demonstrates that no single regulatory model can be considered ideal for all countries. Each approach emerges from a distinct political, economic, and legal cultural context. However, there are interesting patterns to observe. The higher the level of state intervention, as seen in the European Union model, the stronger the legal protection afforded to users. Conversely, the greater the space granted to industry, as in Japan, the greater the level of flexibility and innovation achieved. South Korea and the UK straddle these two poles, developing mechanisms that attempt to balance user protection and digital industry development.

From a legal policy perspective, these findings suggest that the primary debate in metaverse regulation is not about regulation or deregulation, but rather how to establish governance mechanisms that balance technological innovation, human rights protection, and legal certainty. Domestically, the lesson is not to adopt one model in its entirety, but rather to synthesize various best practices emerging globally. This approach is crucial given that Indonesia faces different challenges than those countries, both in terms of institutional capacity, the level of digital literacy , and the development of the national technology ecosystem.

C. Challenges of Jurisdiction and Rule of Law in Virtual Space

Metaverse governance lies not merely in the absence of legal norms, but rather in the inconsistency between the territorial legal paradigm that underpins modern legal systems and the characteristics of virtual space, which is global, decentralized, and without geographical boundaries. For centuries, state jurisdiction has been built on the principle of territorial sovereignty, which grants states the authority to regulate individuals, activities, and legal objects within their territory. However, the development of digital technology, particularly the Metaverse , has created a new reality in which social, economic, and even criminal activities can occur simultaneously across multiple jurisdictions without regard to national borders [37].

applicable law.*law) ,* competent court*jurisdiction*), and the applicable law enforcement mechanisms. However, in the Metaverse , determining these aspects becomes much more complex. As an illustration, a user in Indonesia may experience sexual harassment via avatar by another user domiciled in Canada through a Metaverse platform operated by a United States-based company with servers spread across several countries. This situation raises fundamental questions about which country has the authority to enforce the law and which legal instruments should be applied to such incidents [38].

This complexity shows that the concept *of locus The principle of delicti* , which has long been a primary basis for determining jurisdiction, faces serious challenges in the virtual environment. In traditional legal systems, a crime is generally associated with the physical location where the act was committed or the legal consequences arose. However, in the Metaverse , the act, the consequences, and the technological infrastructure used are often located in different jurisdictions. As a result, the territorial approach that has long been the basis for law enforcement loses its effectiveness when applied to the transnational nature of virtual spaces [39].

This problem is further complicated by the fact that the Metaverse is fundamentally built on digital infrastructure that is not fully under state control. Most Metaverse platforms are developed and operated by global technology corporations, possessing economic capacity, technology, and influence that, in some respects, even surpasses the capabilities of developing countries. This situation creates a phenomenon that some academics refer to as digital *sovereignty*. *dilemma* , namely a situation where the state has a responsibility to protect its citizens, but does not have full control over the digital space where these activities take place [40].

From the perspective of state sovereignty, this phenomenon poses new challenges never before encountered in the conventional legal era. Sovereignty is no longer solely influenced by a state's ability to control its physical territory, but also by its capacity to regulate data flows, digital activities, and global technology platforms. In the context of the Metaverse , the boundaries of sovereignty become increasingly blurred because social interactions no longer depend on geographic location, but rather on access to digital infrastructure largely controlled by non-state actors. As a result, states face difficulties in effectively carrying out regulatory functions without the support of international cooperation or the involvement of digital platforms themselves [41].

Besides jurisdictional issues, another equally important challenge is the issue of evidence and law enforcement. In conventional legal systems, evidence generally consists of documents, witness statements, physical evidence, or electronic recordings that can be verified relatively easily. In contrast, in the Metaverse , much activity takes place in *real time* through avatar interactions , voice communication, virtual body movements, and digital asset transactions stored within complex systems. This situation raises questions about how to accurately identify perpetrators, how to guarantee the authenticity of digital evidence, and how to ensure the chain of custody of evidence . *of custody*) remains intact in the judicial process [42]. Metaverse services and virtual marketplaces in Indonesia are still in the early stages of development. Consumers who conduct digital asset transactions, both in the form of non- fungible tokens (NFT), cryptocurrencies , and in-game assets , face significant legal protection challenges. Law No. 8 of 1999 concerning Consumer Protection provides a normative basis for consumer protection, but does not specifically regulate blockchain- based digital transaction practices and immersive technology [43]. This is in line with the findings of Fitriani, Maulia, and Nugroho (2025) who highlighted the weak reach of the Consumer Protection Law in dealing with foreign business actors [44].

The issue of perpetrator identification becomes increasingly crucial given that most Metaverse platforms allow the use of

pseudonymous or anonymous identities. On the one hand, anonymity is part of the right to privacy and freedom of expression that must be protected. However, on the other hand, anonymity also has the potential to be exploited to commit various forms of legal violations without adequate risk of accountability. This conflict between privacy protection and the need for law enforcement is one of the main dilemmas in modern virtual space governance [45].

The limitations of existing international cooperation mechanisms further exacerbate the situation. Instruments such as *Mutual Legal Assistance* (MLA) and various extradition treaties were primarily designed to address transnational crime in a more conventional context. In practice, these procedures often take a long time, involving complex diplomatic and administrative processes. Yet, violations occurring in the Metaverse occur within seconds and can easily disappear from digital footprints if not promptly addressed. [46] This situation demonstrates the gap between the speed of technological development and the ability of the international legal cooperation system to respond to digital crime.

The Budapest Convention on Cybercrime is often considered one of the most advanced international instruments in facilitating law enforcement cooperation against transnational cybercrime. However, the convention was drafted during a period when the concept of the Metaverse was not yet as developed as it is today. This has resulted in various issues related to virtual identity, digital assets, avatar interactions , and the governance of immersive virtual spaces not being adequately regulated in the instrument [47]. In other words, the current international legal framework still focuses on previous generations of cybercrime and is not fully able to address the complexities presented by the Metaverse .

From a theoretical and normative perspective, this situation demonstrates that the primary challenge facing the Metaverse is not simply a regulatory vacuum, but rather a paradigm crisis in understanding the relationship between law, space, and sovereignty. Modern legal systems have historically been built on the assumption that social and legal space are tied to national territory. However, the Metaverse creates a new social space that can operate independently of geographic boundaries. Consequently, a legal approach that relies solely on territorial principles is no longer adequate to address the emerging challenges [48]. Therefore, new regulations are needed that specifically consider the unique characteristics of digital assets in the Metaverse to ensure optimal protection of user ownership rights. In general, the legal framework governing copyright, electronic transaction security, and virtual asset ownership in this ecosystem still requires improvement. Future legislation must be designed to be more specific and adaptive to keep pace with the rapid dynamics of technology and the realities of the virtual world [49].

In response to this urgency, a paradigm shift is needed from a territory *-based approach. governance*) towards an activity-based approach and protection of rights (*activity-based) governance and rights-based governance*). This approach places user protection at the center of regulation without relying too much on the physical location of the perpetrator or the technological infrastructure used. As a result, the focus of regulation is no longer solely on the question of “where the violation occurred,” but also on “who was harmed,” “what rights were violated,” and “who has the most effective ability to prevent or address the violation” [50].

For Indonesia, the jurisdictional challenges of the Metaverse provide an important lesson: the development of national regulations cannot be undertaken in isolation. Given the global nature of the Metaverse , the effectiveness of national regulations depends heavily on a country's ability to build international cooperation, strengthen digital diplomacy, and promote harmonization of legal standards at the regional and global levels. Without such efforts, various national regulations could potentially lose their effectiveness due to their inability to address digital activities that transcend national sovereignty. Therefore, strengthening cross-border cooperation must be viewed as an integral part of any future Metaverse regulatory strategy.

D. The Adaptive Legal Paradigm as a Model for Metaverse Regulation in Indonesia

A critical review of various international regulatory models shows that the primary challenge in regulating the Metaverse is not simply determining whether countries should implement strict regulations or allow industry freedom, but rather how to develop a legal framework that can adapt to rapid technological change without losing its primary function as an instrument for protecting the rights and interests of the public. In this context, the need for an adaptive legal paradigm becomes increasingly urgent given the dynamic, cross-jurisdictional nature of the Metaverse , which continues to experience unpredictable technological developments.

Efforts to provide legal protection for people active in the digital world require progressive legal reform. This can be achieved by formulating the direction and ideals of metaverse law into policy recommendations and regulations. These rules should not be rigid or merely legal-positivistic, but rather should be responsive legal norms capable of guiding societal behavior [51]. The need for adaptive law is in line with Philippe's ideas. Nonet and Philip Selznick on *Responsive Law* . According to them, law should not be understood solely as a set of rigid and formalistic rules , but must be able to respond to social change, community needs, and new challenges that arise due to developments in the era [52]. In the context of the Metaverse , a legal approach that is only oriented towards the formation of technical and specific rules has the potential to become irrelevant in a short time because technological developments often exceed the speed of the legislative process. Consequently, Indonesia requires a regulatory model that not only functions to address current problems, but is also able to anticipate various risks that may arise in the future.

Based on the results of a comparative analysis of the European Union, the United Kingdom, South Korea, and Japan, this study proposes an adaptive legal paradigm built on four main principles, namely technology *neutrality , human-centric governance , platform accountability* ,and *cross -border cooperation . These four principles are not intended as stand-alone norms, but rather as conceptual foundations that can be used in formulating national legal policies related*

to Metaverse governance .

The first principle is *technology Neutrality* . This principle emphasizes that regulations should not be based on a specific type of technology, but rather on the legal and social impacts of the use of that technology [53]. An approach that is too technology-oriented often results in regulations becoming outdated quickly because technological developments occur faster than the process of law formation. In the context of the Metaverse , regulations that focus solely on a particular platform or technology have the potential to lose their relevance when new innovations emerge with different characteristics. Therefore, laws need to be designed based on general principles that remain applicable despite technological changes.

technology principles *Neutrality* is crucial for Indonesia, given that the national digital ecosystem is still in its infancy. Overly specific regulations can stifle innovation and reduce the competitiveness of the domestic technology industry. Conversely, principles-based regulations allow the country to maintain flexibility without sacrificing legal certainty. With this approach, the regulatory focus is directed at protecting the rights and interests of users, rather than the technology used to provide the services.

The second principle is *human- centric governance* . This principle stems from the view that humans must remain at the center of the entire process of developing and utilizing digital technology [54]. In many cases, discourse on the Metaverse tends to be dominated by discussions of technological innovation, economic opportunities, and investment potential, while aspects of protecting user rights are often placed in a secondary position. In fact, the primary goal of regulation should not only encourage the growth of the digital economy, but also ensure that technological development does not sacrifice human dignity, the right to privacy, freedom of expression, or the right to a sense of security.

At the national level, this principle holds high relevance, given that the constitution places human rights protection as one of the primary objectives of state governance. Any policy related to the Metaverse must consider aspects of personal data protection, user security, prevention of digital discrimination, protection of vulnerable groups, and mitigation of psychological risks that can arise from intensive virtual interactions. Therefore, Metaverse regulations serve not only as an instrument for controlling technology but also as a means of protecting human values in the digital age.

The third principle is *platform accountability* . The development of the Metaverse demonstrates that digital platforms play a significant role in shaping user behavior through their technological design, algorithms, moderation systems , and internal policies. In many cases, platforms no longer merely serve as providers of technological infrastructure but have become actors with significant influence over users' social lives [55]. Therefore, the approach of positioning platforms as neutral parties with no responsibility for the activities occurring within their systems is becoming increasingly difficult to maintain.

The principle *of platform accountability requires that* Metaverse operators have a proportional obligation to prevent, detect, and address various forms of violations occurring within their platforms. This obligation can be realized through the provision of easily accessible reporting mechanisms, transparent moderation systems , victim protection, and regular risk audits of the technology used. This approach aligns with global regulatory developments that increasingly demand accountability from technology companies for the social impacts of their digital services.

The fourth principle is *cross -border cooperation* . Of all the challenges discussed previously, jurisdictional issues are the most difficult to resolve through national regulations alone. The cross-border nature of the Metaverse means that the effectiveness of national law is highly dependent on a country's ability to build international cooperation [56]. Therefore, strengthening digital diplomacy and harmonizing international regulations must be an integral part of Indonesia's Metaverse regulatory strategy . Cross-border cooperation can be achieved through various mechanisms, such as bilateral agreements, ASEAN regional cooperation, active participation in global internet governance forums, and the development of international standards for protecting Metaverse users . Furthermore, Indonesia needs to encourage the establishment of mechanisms for exchanging information and digital evidence more quickly than conventional *Mutual Legal Assistance* (MLA) procedures, which have been deemed ineffective in addressing real-time *digital crimes* .

Based on these four principles, Indonesia should not adopt an overly strict regulatory approach as implemented by the European Union or a *laissez-faire approach*. which leaves regulation entirely to industry. A more realistic option is to develop a *co-regulation model that combines the roles of the state, industry, academia, and civil society in building inclusive and adaptive* Metaverse governance . This approach allows the state to maintain its legal protection function without hindering technological innovation, one of the driving forces of the national digital economy.

Ultimately, the adaptive legal paradigm proposed in this study serves not only as a regulatory recommendation for the Metaverse but also as a conceptual framework that can be used to address various forms of future digital technology. Through a *technology- based approach, neutrality , human- centric governance , platform accountability* , and *cross -border cooperation* , Indonesia has the opportunity to build a more responsive, progressive, and sustainable legal system in the face of global digital transformation.

Conclusion

The development of the Metaverse has created a new digital interaction space that presents both significant opportunities and complex legal challenges, particularly because conventional legal systems have not been fully able to keep up with the acceleration of technological innovation that has given rise to various forms of legal anomie, such as unclear regulations regarding digital identity, virtual harassment, biometric data protection , and platform accountability. Research results show

that each country is developing different regulatory approaches in response to the development of the Metaverse , ranging from strict regulatory models to more flexible and collaborative approaches, so that no single regulatory model can be applied universally. Furthermore, the cross-border nature of the Metaverse poses serious challenges to the concepts of jurisdiction and the rule of law that have long been the foundation of the modern legal system. Therefore, Indonesia requires an adaptive legal paradigm that can accommodate technological dynamics while guaranteeing the protection of user rights through the application of *technology principles*. *neutrality* , *human- centric governance* , *platform accountability* , and *cross -border cooperation , so as to create responsive, equitable, and sustainable* Metaverse governance in facing future digital transformation.

Acknowledgement

The author expresses his sincerity appreciation to all parties who have contributed to the research process and writing of this article . I express my deepest gratitude to my supervisors for their continuous guidance , motivation , and assistance from the beginning to the end of this work . Without their support , this research would not have been completed successfully . I also express my gratitude to my beloved family and friends who have provided constant encouragement , attention , and understanding throughout this process .

References

[1] M. Ball, The Metaverse: And How It Will Revolutionize Everything. New York, NY, USA: Liveright Publishing Corporation, 2022.
[2] N. F. Gunawan et al., "Metaverse as Transformation and Innovation in Education in the Digital Era," Hipkin Journal of Educational Research, vol. 1, no. 2, 2024, doi: 10.64014/hipkin-jer.v1i2.12.
[3] L. Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford, U.K.: Oxford University Press, 2014.
[4] B. Z. Tamanaha, A General Jurisprudence of Law and Society. Oxford, U.K.: Oxford University Press, 2001.
[5] É. Durkheim, The Division of Labor in Society. New York, NY, USA: Free Press, 1997.
[6] D. J. B. Svantesson, Solving the Internet Jurisdiction Puzzle. Oxford, U.K.: Oxford University Press, 2017.
[7] European Parliament and Council, "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)," 2022.
[8] UK Parliament, Online Safety Act 2023, Chapter 50, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/2023/50
[9] S.-Y. Yoon, "Ethics Guidelines for Metaverse Released by Korea's Science and ICT Ministry," Korea JoongAng Daily, Nov. 28, 2022. [Online]. Available: https://koreajoongangdaily.joins.com/business/ethics-guidelines-for-metaverse-released-by-koreas-science-and-ict-ministry/10200031
[10] Y. Kunitake and L. Bredikhina, "Discussions on the Legal Policies in the Metaverse: From the Perspective of Diversifying Self-Expression," 2024. [Online]. Available: https://sdgs.un.org/sites/default/files/2024-05/Kunitake%3B%20Bredikhina_Discussions%20on%20the%20Legal%20Policies%20in%20the%20Metaverse.pdf
[11] P. M. Marzuki, Penelitian Hukum. Jakarta, Indonesia: Kencana, 2011.
[12] European Parliament and Council, "Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act)," 2022; European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," COM(2021) 206 Final, 2021; UK Parliament, Online Safety Act 2023, 2023.
[13] K. Zweigert and H. Kötz, An Introduction to Comparative Law. Oxford, U.K.: Oxford University Press, 1998.
[14] J. Ibrahim, Teori dan Metodologi Penelitian Hukum Normatif. Malang, Indonesia: Bayumedia Publishing, 2019.
[15] K. Krippendorff, Content Analysis: An Introduction to Its Methodology, 4th ed. Thousand Oaks, CA, USA: Sage Publications, 2018.
[16] P. M. Hadjon and T. S. Djatmiati, Argumentasi Hukum. Yogyakarta, Indonesia: Gadjah Mada University Press, 2020.
[17] M. Ball, The Metaverse: And How It Will Revolutionize Everything. New York, NY, USA: Liveright Publishing Corporation, 2022.
[18] É. Durkheim, The Division of Labor in Society. New York, NY, USA: Free Press, 1997.
[19] P. Olson, "Meta Opens Investigation After Woman Reports Being Groped in Virtual Reality," Bloomberg, Dec. 17, 2021. [Online]. Available: https://www.bloomberg.com/opinion/articles/2021-12-15/the-metaverse-via-oculus-is-awkward-if-you-re-a-woman-and-beware-of-griefers
[20] L. Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford, U.K.: Oxford University Press, 2014.
[21] J. Bailenson, Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do. New York, NY, USA: W. W. Norton & Company, 2018.
[22] D. J. Solove, Understanding Privacy. Cambridge, MA, USA: Harvard University Press, 2008.
[23] M. Madary and T. K. Metzinger, "Real Virtuality: A Code of Ethical Conduct," Frontiers in Robotics and AI, vol. 3, 2016, doi: 10.3389/frobt.2016.00003.
[24] D. J. B. Svantesson, Solving the Internet Jurisdiction Puzzle. Oxford, U.K.: Oxford University Press, 2017.
[25] L. Lessig, Code and Other Laws of Cyberspace. New York, NY, USA: Basic Books, 2006.
[26] J. E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford, U.K.: Oxford University Press, 2019.
[27] P. Nonet and P. Selznick, Law and Society in Transition: Toward Responsive Law. New Brunswick, NJ, USA: Transaction Publishers, 2001.
[28] European Parliament and Council, "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)," 2022.
[29] European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," COM(2021) 206 Final, 2021.
[30] F. A. M. Magalhães and I. M. Calle, "Consumer Protection in the Digital Age: A Reflection on Regulation 2022/2065 (Digital Services Act—DSA) and Agenda 2030," in A Digital Europe for Citizens: Data Governance, Data Markets, Data Services. Cham,

Switzerland: Springer, 2025.
[31] G. Dimita et al., IP and Metaverse(s): An Externally Commissioned Research Report, Queen Mary Law Research Paper No. 427, 2024. [Online]. Available: https://papers.ssrn.com/
[32] UK Parliament, Online Safety Act 2023, Chapter 50, 2023.
[33] S.-Y. Yoon, "Ethics Guidelines for Metaverse Released by Korea's Science and ICT Ministry," Korea JoongAng Daily, Nov. 28, 2022.
[34] A. Oriishi and Y. Kunitake, "Comparative Soft-Law Principles for the Metaverse: Balancing Governance and Creator Inclusion," in TPRC 53 Research Conference on Communications, Information and Internet Policy, 2025. [Online]. Available: https://www.researchgate.net/publication/394263221
[35] Y. Kunitake and L. Bredikhina, "Discussions on the Legal Policies in the Metaverse: From the Perspective of Diversifying Self-Expression," 2024. [Online]. Available: https://www.researchgate.net/publication/381375952
[36] Y. Tsuji, "Regulations on Japanese Video Games for Protection of Children," in Japanese Video Game Regulation Studies, 2018. [Online]. Available: https://journals.library.columbia.edu/index.php/cjal/article/view/3364
[37] D. J. B. Svantesson, Solving the Internet Jurisdiction Puzzle. Oxford, U.K.: Oxford University Press, 2017.
[38] B. Bayaraa et al., "Jurisdictional Challenges in Metaverse," in Tech Fusion in Business and Society: Harnessing Big Data, IoT, and AI, 2025, pp. 229–239, doi: 10.1007/978-3-031-84636-6_19.
[39] C. Ryngaert, Jurisdiction in International Law. Oxford, U.K.: Oxford University Press, 2015.
[40] J. E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford, U.K.: Oxford University Press, 2019.
[41] J. Daskal, "The Un-Territoriality of Data," Yale Law Journal, vol. 125, no. 2, pp. 326–398, 2015. [Online]. Available: https://yalelawjournal.org/article/the-un-territoriality-of-data
[42] O. S. Kerr, Computer Crime Law. St. Paul, MN, USA: West Academic Publishing, 2021.
[43] I. R. W. Putra et al., "Bought and Lost: Perlindungan Hukum bagi Konsumen atas Kehilangan Aset Digital di Era Metaverse," Jurnal Hukum, Politik dan Ilmu Sosial, vol. 4, no. 3, Sep. 2025, doi: 10.55606/jhpis.v4i3.5587.
[44] M. Fitriani, I. Maulia, and L. Dafira, "Perlindungan hukum terhadap konsumen dalam transaksi e-commerce lintas negara," Al-Zayn: Jurnal Ilmu Sosial & Hukum, vol. 3, no. 3, pp. 1387–1397, 2025, doi: 10.61104/alz.v3i3.1323.
[45] D. J. Solove, Understanding Privacy. Cambridge, MA, USA: Harvard University Press, 2008.
[46] M. U. Asghar, M. H. Javed, and S. Azhar, "The Regulation of Cybercrime in International Law: Discussing the Legal Frameworks and Challenges in Regulating Cybercrime," Indus Journal of Social Sciences, vol. 3, no. 2, pp. 417–430, 2025, doi: 10.59075/ijss.v3i2.1267.
[47] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185, 2001. [Online]. Available: https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf
[48] R. Brownsword, Law, Technology and Society: Re-imagining the Regulatory Environment. London, U.K.: Routledge, 2019.
[49] T. Dragono et al., "Perlindungan Aset Digital Dalam Dunia Metaverse Berdasarkan Hukum Nasional," Jurnal Kewarganegaraan, vol. 7, no. 1, Jun. 2023, doi: 10.31316/jk.v7i1.4901.
[50] P. Muli, "Jurisdiction in the Metaverse: Rethinking Territoriality in International Law," Cyberspace Law eJournal, May 22, 2026. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6772759
[51] D. Ambarwati, "Urgensi Pembaharuan Hukum di Era 'Metaverse' dalam Perspektif Hukum Progresif," Jurnal Dialektika, vol. 7, no. 2, Sep. 2022, doi: 10.36636/dialektika.v7i2.1306.
[52] P. Nonet and P. Selznick, Law and Society in Transition: Toward Responsive Law. New Brunswick, NJ, USA: Transaction Publishers, 2001.
[53] R. Brownsword, Law, Technology and Society: Re-imagining the Regulatory Environment. London, U.K.: Routledge, 2019.
[54] L. Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford, U.K.: Oxford University Press, 2014.
[55] L. Lessig, Code and Other Laws of Cyberspace. New York, NY, USA: Basic Books, 2006.
[56] D. J. B. Svantesson, Solving the Internet Jurisdiction Puzzle. Oxford, U.K.: Oxford University Press, 2017.