International Metaverse Association

Metaverse Convergence Research Institute

ISSN 3059-0442

Journal of Virtual Convergence Research

Volume 1 Number 3 Jul. 2025

Received: 30 April 2025. Accepted: 01 June 2025

Journal of Virtual Convergence Research
2025, VOL. 1, NO. 3, 1~46.
https://intlmetaverse.com/home/journal?lang=en

International Metaverse Association &
Metaverse Convergence Research Institute

Multiple identities in the metaverse: An exploratory study on ethical challenges and legal regulatory directions (A case study approach)

Seonah Moon[1,*], Inhoi Kim[1]

[1] Ph.D. Student, Graduate School of Metaverse, Sogang Univ., Korea

[*] Corresponding author: Seonah Moon. Email: seonahmoon@sogang.ac.kr

Abstract

This study examines the impact of multiple identities formed within the metaverse on user experiences and social interactions, while critically addressing the ethical dilemmas and legal challenges that emerge as a result. Through a multiple case study analysis of platforms such as Roblox, Horizon Worlds, and Zepeto, along with the widely discussed Patel incident, the research categorizes key issues including identity theft, privacy violations, deceptive conduct, and virtual sexual harassment. It then assesses the limitations of current legal frameworks in regulating such phenomena. Based on these findings, the paper proposes regulatory directions that include the expansion of legal definitions for non-physical acts, the implementation of identity verification systems, and the enhancement of data protection mechanisms.

Keywords : Multiple identities, Metaverse legislation, Digital ethics,
Virtual environment regulation

Multiple identities in the metaverse: An exploratory study on ethical challenges and legal regulatory directions (A case study approach)

1. Introduction

1.1 Research Background

The metaverse constitutes a digital ecosystem where users can explore and construct diverse identities beyond the limitations of the physical world. The phenomenon of multiple identities—where a single individual expresses or maintains different personas depending on the context—functions as a powerful tool for self-exploration and the expansion of social interaction. However, this very multiplicity also serves as a source of ethical and legal conflicts, such as identity theft and privacy violations. Focusing on representative cases including the Patel incident and Roblox, this study aims to examine both the opportunities and threats associated with multiple identities in the metaverse and to propose regulatory responses suited to this emerging environment.

1.2 Research Objectives and Research Questions

This study aims to analyze the formation of multiple identities in the metaverse and the resulting ethical and legal challenges, with the goal of proposing effective legal and regulatory responses. While highlighting the freedom of self-expression and the opportunities for social interaction that multiple identities afford users, this research also

seeks to critically examine the conflicts and limitations that arise from such dynamics. Accordingly, the study is guided by the following research questions:

- Formation of Multiple Identities – How are multiple identities formed within the metaverse, and how do they influence user experience and social interaction?
- Ethical Conflicts and Legal Issues – What are the key factors through which multiple identities lead to ethical and legal problems such as privacy violations, identity theft, and deceptive behavior?
- Limitations of the Current Legal System – How does the existing legal framework address these issues, and where does it fall short? How can regulation be designed to preserve the benefits of multiple identities while minimizing potential misuse?

1.3 Scope and Limitations of the Study

This research focuses on analyzing ethical and legal issues related to the misuse of identity within prominent metaverse platforms such as Roblox, Zepeto, and Horizon Worlds. The study does not include empirical methods such as user interviews or survey-based approaches; instead, it emphasizes case-based analysis to derive regulatory implications.

Differences in technical infrastructure and user environments across platforms, as well as the diversity of national legal systems, pose certain limitations to the analysis. While the study draws primarily on examples from South Korea, the United States, and the European Union, it does not encompass the full global spectrum of regulatory contexts.

Moreover, due to the rapid evolution of metaverse technologies and associated ethical standards, some findings may be constrained by future technological developments. Nevertheless, this study offers a balanced perspective on the opportunities and risks inherent in multiple identities in the metaverse and provides a meaningful starting point for legal and policy discussions aimed at user protection and the restoration of trust.

2. Theoretical Background

2.1 Overview of the Metaverse

The metaverse is an immersive digital ecosystem that integrates cutting-edge technologies such as virtual reality (VR), augmented reality (AR), and artificial intelligence (AI). It offers users a space in which to transcend physical limitations, explore diverse identities, and form complex social relationships. By simulating real-world social structures, the metaverse enables users to engage in new types of social experiences and psychological immersion through their virtual selves (Garon, 2008).

Prior studies have shown that identity within virtual environments like the metaverse is inherently multilayered, allowing users to fluidly explore multiple roles and selves across various contexts (Donath, 1999; Turkle, 1995). Such environments expand the modes of self-expression available to individuals and serve as a foundation for the development of multiple identities.

In this respect, the metaverse functions not merely as a technological platform, but as a dynamic social space that facilitates identity experimentation and interaction. It is emerging as a novel digital arena that satisfies users' psychological needs for self-exploration as well as their social needs for connection and engagement.

2.2 Concept and Mechanisms of Multiple Identities

Multiple identities refer to an individual's capacity to express different versions of the self either simultaneously or sequentially, depending on the context or environment. Wearing (2011) conceptualized this phenomenon as a psychological and social resource that enables individuals to perform various roles and explore distinct aspects of their identity across diverse social situations. In digital environments such as the metaverse—where physical constraints are absent—these identity expressions become significantly more fluid and unconstrained (Donath, 1999; Turkle, 1995).

Prior research suggests that multiple identities in the metaverse exhibit four key characteristics. First, contextual dependency. Users adapt and express different identities depending on the activity—whether it be work, gaming, or social interaction. Identity is not fixed, but dynamically shaped by situational factors and environmental cues (Garon, 2008).

Second, simultaneity and switchability. Within the metaverse, users can maintain

multiple identities concurrently or shift between them at will. This flexibility allows individuals to experiment with diverse social roles and select identities that best fit specific interactions (Turkle, 1995).

Third, self-exploration and expression. The metaverse provides a unique space for users to experiment with identities that may be difficult to explore in the real world, fostering psychological satisfaction and a sense of self-efficacy (Donath, 1999). This process is often accompanied by a sense of personal expansion and psychological liberation.

Fourth, digitally optimized identity performance. Identities in the metaverse are manifested through avatars, interfaces, and behavioral logs, which are inherently shaped by the technological architecture of the platform. This allows for more creative, adaptable expressions of selfhood.

Moreover, virtual identities can be linked to users' actual selves through visual representation, linguistic behavior, and social responses (Alsarkal et al., 2015). These signals play a role in influencing others and in the construction of social trust (De Zwart & Lindsay, 2009). Turkle (1995) emphasized that such identity experimentation fosters the learning of new social norms and broadens the scope of social interaction.

In conclusion, multiple identities serve as a central concept in enhancing user

experience and expanding social connectivity within the metaverse. However, they also raise ethical and legal concerns, such as identity theft and privacy violations. As such, a balanced and nuanced understanding of the dual nature of multiple identities is essential.

2.3 Multiple Identities in the Metaverse: Ethical Conflicts and Duality

While multiple identities in the metaverse enable users to explore the self and engage in enriched social interactions, they also carry inherent risks stemming from the anonymity and fluidity of identity that characterize virtual environments (Garon, 2008). The freedom to experiment with identity may enhance creativity and autonomy, but it can equally lead to breaches of social trust and unethical behavior.

The ethical dilemmas associated with multiple identities can be broadly categorized into five major areas. First, identity theft. Due to the flexible nature of identity representation in the metaverse, users may imitate the avatars or profiles of others, particularly when virtual identities are linked to real-world identities. In the case of Roblox, for example, fraudulent actors exploited the trust of minors by impersonating other users to propose fake transactions—highlighting how digital impersonation can result in tangible harm (van Kokswijk, 2007).

Second, privacy violations. User interactions in the metaverse—such as

conversations, behavioral data, and avatar activity logs—are often collected and utilized without proper consent by platform providers or third parties. This reflects a significant gap in data protection and raises urgent questions about platforms' responsibilities in safeguarding personal information (Naseh, 2016).

Third, deceptive behavior. Multiple identities may be misused for deceptive purposes, such as false identity construction or avatar-based impersonation. Some users exploit this flexibility to gain financial advantage, extract sensitive information, or provoke social disruption. Such actions undermine trust and diminish the overall quality and safety of interactions in virtual spaces (de Zwart & Lindsay, 2009).

Fourth, identity diffusion and alienation. Although the metaverse offers opportunities for self-exploration, excessive divergence between real and virtual identities may cause psychological confusion or social detachment. Turkle (1995) warned that immersive digital environments, while empowering in terms of identity experimentation, may lead individuals to experience fragmented or disoriented senses of self if overly immersed.

Fifth, anonymity and moral disengagement. While anonymity is essential for expressive freedom, it can also enable users to evade accountability and engage in unethical behavior. Shielded by digital invisibility, users may engage in hate speech,

harassment, or aggressive conduct—thereby undermining the constructive potential of identity experimentation (Parmentier & Rolland, 2009).

These ethical conflicts are not merely theoretical but have manifested in real-world cases. A prominent example is the Patel incident, a case of virtual sexual harassment on a Meta platform in which the victim experienced psychological and even physiological distress comparable to that caused by real-world offenses. This case underscores the necessity of applying ethical and legal standards in virtual spaces with the same rigor as in physical ones.

2.4 Legal Issues Related to Multiple Identities in the Metaverse

The metaverse provides users with a space to experiment with identity and engage in novel forms of social interaction. However, the fluidity and anonymity inherent in multiple identities pose significant legal challenges that existing legal frameworks are ill-equipped to address. This section identifies four primary legal issues related to multiple identities in the metaverse and discusses the limitations of current legal systems and directions for improvement.

First, identity theft and limitations of legal accountability. In the metaverse, users frequently impersonate others by replicating their avatars, nicknames, or visual characteristics to gain trust and perpetrate fraud or deception—such as the well-known

Roblox case. However, since current legal systems do not recognize virtual identities as independent legal entities, impersonation in virtual settings is less likely to result in legal penalties or effective remedies compared to real-world identity theft (Naseh, 2016). The inability to authenticate identities and track users further hampers investigation and post-incident responses. This highlights the need for a new legal framework specifically designed to protect digital identities, with clear definitions and enforceable sanctions.

Second, privacy violations and regulatory gaps in data protection. Metaverse platforms collect extensive personal data from users, including conversations, geolocation, and behavioral patterns. However, this data is often gathered without explicit consent or transparent explanation of its use. Such practices infringe upon users' right to informational self-determination and raise concerns about the commercial exploitation of sensitive data by platforms. Although international standards like the GDPR offer some guidance, inconsistencies between national legal systems and the unique technical architecture of the metaverse hinder uniform enforcement. Thus, global-level data protection regulations that apply to metaverse environments and ensure users' ownership and control over their data are urgently needed.

Third, anonymity and evasion of legal responsibility. The metaverse frequently

enables unethical or unlawful behavior—such as sexual harassment, deception, or hate speech—under the guise of anonymity. The Patel incident exemplifies this issue, where the victim experienced psychological harm comparable to real-life trauma, yet the perpetrator avoided legal consequences due to the difficulty of verifying identity. This case demonstrates the urgent need to redefine the legal interpretation of non-physical actions and establish clear criteria for liability in virtual spaces. Implementing identity registration and verification systems that limit the abuse of anonymity, while preserving user privacy, is essential (de Zwart & Lindsay, 2009). Furthermore, assigning responsibility to platform operators for overseeing anonymity practices is a critical step toward rebuilding trust and establishing ethical usage norms (Naseh, 2016).

Fourth, legal jurisdiction and international regulatory voids. The metaverse constitutes a transnational digital ecosystem where users and platforms often fall under different jurisdictions. As a result, it is often unclear which national laws apply when crimes occur, and international legal cooperation tends to be slow or insufficient (van Kokswijk, 2007). The situation becomes more complex when virtual identities operate as autonomous or semi-automated agents, blurring the lines of accountability between users and platforms. These challenges call for the establishment of international legal cooperation frameworks and globally recognized digital jurisdiction protocols to effectively govern metaverse-

related incidents.

2.5 Limitations of Previous Research and the Contribution of This Study

Previous studies have primarily focused on the positive aspects of multiple identities in the metaverse, emphasizing their role in enabling personal self-exploration and facilitating social interaction. For instance, Turkle (1995) highlighted how users could experiment with different personas within virtual environments such as MUDs, leading to psychological satisfaction and identity growth. Similarly, Donath (1999) argued that online identities function as social signals, contributing to relationship formation and the development of trust. However, these studies often failed to address the ethical dilemmas and legal challenges that may arise from the use and abuse of multiple identities in virtual environments, nor did they provide concrete strategies for managing such issues.

Moreover, the bulk of existing literature has remained theoretical or conceptual, lacking empirical analysis grounded in real-world cases such as identity theft, privacy breaches, deceptive behaviors, and the exploitation of anonymity. Particularly absent are legal discussions concerning structural deficiencies exposed by incidents like the Patel case, where the victim experienced tangible psychological harm but legal recourse remained elusive due to the limitations of current laws. This gap underscores the need for more practice-oriented research that accounts for the technological and sociocultural complexity

of the metaverse.

This study seeks to address these gaps and offers three key contributions. First, it presents a balanced analysis of the dual nature of multiple identities in the metaverse—highlighting both the positive functions (e.g., self-expression and the expansion of social capital) and the negative consequences (e.g., ethical conflicts and legal evasion). Through case-based analysis, it concretizes the risks associated with these digital identity practices.

Second, it proposes actionable legal and regulatory solutions. By focusing on pressing issues such as identity theft, privacy violations, deception, and jurisdictional ambiguity, this study critiques the limitations of existing legal frameworks and offers specific regulatory recommendations—such as identity registration systems, enhanced platform accountability, and international legal cooperation.

Third, it delivers policy-relevant and practice-oriented implications. Moving beyond theoretical insights, this study provides practical guidelines and a regulatory framework that platform operators and policymakers can apply to foster a more sustainable, trustworthy, and accountable metaverse ecosystem.

3. Research Methodology

This study adopts a case study approach to explore multiple identities within the

metaverse and the ethical challenges and legal regulatory needs associated with them. Case studies are particularly useful for gaining an in-depth understanding of complex social phenomena and are well-suited for identifying the root causes of issues and potential solutions through the analysis of real-world incidents. By conducting case analyses, this research seeks to examine the formation and misuse of multiple identities and, based on these findings, propose ethical resolutions and legal regulatory frameworks.

3.1 Case Study Design

This study employs a multiple case study approach to conduct a comparative analysis of various instances of identity exploitation within metaverse platforms. Each case is selected based on its relevance to real-world occurrences, with a focus on highlighting the dual nature of multiple identities and identifying their associated legal and ethical concerns.

The research design consists of the following key phases.

- Case Selection – Identifying notable cases of identity theft, privacy violations, deceptive practices, and virtual harassment that have occurred within metaverse platforms.
- Data Collection – Gathering detailed information on each case through literature reviews, news articles, legal documents, and relevant reports.
- Application of an Analytical Framework – Structuring case analysis into key dimensions, including incident background, stakeholders, ethical and legal

concerns, and responses from platforms and legal authorities.

- Comparative and Synthesis Analysis – Comparing commonalities and differences across cases to derive insights into the dual nature of multiple identities and the necessity for legal regulations.

By applying this structured case study approach, this research aims to provide a comprehensive understanding of the ethical and legal complexities surrounding multiple identities in the metaverse, offering practical regulatory recommendations for digital governance.

3.2 Case Selection Criteria and Analytical Framework

3.2.1 Case Selection Criteria

This study selects key incidents within the metaverse based on the following criteria.

- Relevance to Multiple Identities – The selected cases must involve issues related to multiple identities, such as identity theft, deceptive behavior, or privacy violations.
- Social and Legal Significance – The cases must have substantial social impact, highlighting the need for legal discourse and regulatory intervention.
- Platform Diversity – The study includes cases from a variety of metaverse platforms (e.g., Roblox, Horizon Worlds, and Zepeto) to reflect platform-specific characteristics.
- Data Accessibility – The cases must have sufficient available data, including documents, reports, and news sources, to allow for comprehensive analysis.

3.2.2 Case Analysis Framework

To ensure a systematic examination of each case, this study employs a six-step analytical framework.

- Case Overview – Identifying the platform, timeline, background, and progression of events.
- Key Stakeholders – Analyzing the roles of the victim (age, gender, type of activity), perpetrator (degree of anonymity, motivation), and platform operators.
- Types of Ethical and Legal Issues – Categorizing the specific nature of violations, such as identity theft, privacy infringement, deceptive practices, and virtual harassment.
- Root Cause Analysis – Examining factors contributing to the incident, including platform design flaws, user anonymity, and legal loopholes.
- Response Analysis – Evaluating initial platform responses, legal actions, the applicability of existing laws, and their limitations.
- Proposed Solutions – Suggesting ethical resolutions and legal regulatory directions based on case findings.

3.3 Data Collection and Analysis Methods

This study employs a qualitative research approach based on case studies, utilizing multiple sources for data collection and structured analysis.

3.3.1 Data Collection Methods

- Literature Review – Establishing a theoretical foundation for multiple identities in the metaverse through existing research, academic papers, reports, and legal documents.
- Case Data Collection – Gathering detailed case information from news articles,

official platform reports, legal records, and online community discussions.

- Policy and Records Analysis – Examining platform policy documents and user agreements to assess incident response mechanisms and regulatory limitations.

3.3.2 Data Analysis Methods

The collected data is examined using content analysis and comparative analysis to derive meaningful insights.

- Content Analysis – Identifying patterns and key themes by analyzing the causes, ethical and legal issues, and platform responses associated with each case.
- Comparative Analysis – Comparing commonalities and differences across cases to highlight the dual nature of multiple identities in the metaverse and to identify possible solutions.
- Synthesis Analysis – Consolidating findings to clarify the root causes of ethical conflicts, assess the limitations of existing legal frameworks, and propose improvements.

Through this systematic approach, the study aims to provide a comprehensive understanding of multiple identities in the metaverse and offer practical regulatory insights to mitigate associated risks.

4. Case Study Findings

This study examines four notable cases of ethical and legal issues within metaverse platforms—Roblox, Horizon Worlds, Zepeto, and the Patel incident—to analyze the causes,

consequences, and platform responses. By conducting an in-depth analysis of these cases, this study highlights the dual nature of multiple identities, identifies ethical dilemmas, and reveals regulatory gaps in the existing legal framework.

4.1 Case 1: Identity Theft in Roblox

Roblox is a globally popular metaverse-based gaming platform that allows users to create custom avatars and engage with various forms of content. However, this open and creative environment has also given rise to a serious ethical issue—identity theft.

Many users have impersonated others' avatars to gain trust, subsequently engaging in fraudulent transactions or hijacking accounts through deceptive practices. This issue has been particularly prevalent among younger users, who, as victims, have suffered not only financial losses but also psychological distress.

The Roblox case illustrates that identity theft within virtual spaces is not merely a digital crime but one that can lead to real-world monetary damages. Moreover, the platform's inadequate response mechanisms and the perpetrators' ability to exploit anonymity raise fundamental concerns about the safety of metaverse environments.

This case clearly demonstrates that unless metaverse platforms establish fundamental solutions for identity management, ensuring user protection and building trust will remain a

challenge. To effectively address identity theft, it is crucial to implement platform-level identity authentication systems and strengthen legal enforcement measures against identity fraud.

Table 1. *Identity Theft Issues Roblox*

Case Overview	Platform	Roblox (Metaverse-based game platform)
	Background	While users are free to create avatars and interact with others, incidents of identity theft and trust exploitation through avatar impersonation have occurred frequently.
	Major Stakeholders	Victims: Primarily minor users, who have suffered from financial fraud or account hijacking. Perpetrators: Exploit anonymity to imitate victims' avatars and identities, engaging in deceptive practices. Platform Operators: Delayed issue resolution due to the absence of an effective initial response system.
Ethical & Legal Problem Analysis	Problem types	Identity Theft: Perpetrators mimic user avatars to gain trust, then propose fraudulent transactions or seize accounts. Deceptive Practices: Collect victims' account credentials through fraudulent links.
	Cause of the Problem	Challenges in User Verification: Difficulty in identifying users due to anonymity. Weak Reporting and Response System: Ineffective complaint mechanisms and inadequate follow-up measures.
	Platform Response and Legal Limitations	Roblox provides a reporting feature and blocking system, but response times are delayed, and victim restitution remains insufficient. Legal Involvement: Most incidents are handled internally by the platform, making it difficult to pursue legal prosecution or formal penalties.
Victims and social impacts	Victim Experience: Financial losses, psychological stress, and disruptions in platform activity due to account hijacking. Social Ramification: Erosion of user trust and heightened concerns regarding platform security.	
Proposed Improvement	Platform Improvements: ● Strengthening identity verification systems and introducing transaction authentication mechanisms. ● Improving the efficiency of the reporting process and enhancing victim support measures. Legal and Regulatory Recommendations: ● Clearly defining identity theft within digital spaces and reinforcing legal sanctions against digital crimes. User Education:	

	• Implementing digital security and ethics education programs tailored for minor users.

4.2 Case 2: Privacy Violations in Horizon Worlds

Horizon Worlds, developed by Meta, is a social VR metaverse platform that allows users to interact in real-time and engage in various activities within a fully immersive virtual environment. However, this highly immersive nature has led to significant privacy concerns, raising critical ethical and legal issues.

As summarized in Table 2 Privacy Violations in Horizon Worlds, this case involved the unauthorized collection of sensitive user data, including conversation logs, behavioral patterns, and location data, without explicit user consent. Furthermore, there were allegations that the collected data was leaked for commercial use, triggering widespread controversy. The platform's failure to implement robust data protection measures and its opaque privacy policies severely eroded user trust and exposed fundamental structural flaws in data governance within the metaverse.

This case illustrates that privacy violations in metaverse environments are not merely technological issues but critical ethical challenges exacerbated by legal loopholes. It underscores the urgent need for comprehensive regulations to safeguard user data and transparent data management systems within metaverse platforms.

Table 2. *Privacy Violations in Horizon Worlds*

Case Overview	Platform	Horizon Worlds (Meta's VR Metaverse Platform)
	Background	A case was reported where user conversations and behavioral data were collected without consent and exploited for commercial purposes.
	Major Stakeholders	Victims: Platform users who experienced personal data breaches and privacy violations. Platform Operators: Lack of robust data management systems and insufficient transparency in handling user data.
Ethical & legal Problem Analysis	Problem Types	Invasion of Privacy: User data (conversations, behavioral records) was collected without consent and used for commercial purposes.
	Cause of the Problem	Platform's data collection policies were unclear, and users were unaware of how their information was being used. Weak data security systems exposed user data to potential breaches.
	Platform Response & Legal Limitations	The platform partially revised its privacy policies, but effective data protection measures remained inadequate. In countries where strict regulations like GDPR do not apply, legal responses were even more limited.
Victims & Social Impacts	Victims' Experience: Users experienced anxiety and a loss of trust due to the exposure of their personal data. Social Ramifications: Public distrust in the platform grew, fueling broader discussions on data protection and privacy rights.	
Proposed Improvements	Platform Improvements: ● Strengthening transparency and explicit user consent procedures for data collection. ● Enhancing data security measures and implementing stronger user information protection systems. Legal and Regulatory Recommendations: ● Applying international data protection regulations, such as GDPR, to a metaverse platform. Strengthening user rights: • The right to access personal data collected by platforms and the right to request data deletion to protect personal privacy	

The Horizon Worlds case highlights the critical importance of transparency in data collection and user privacy protection within metaverse platforms. When platforms fail to uphold stringent privacy measures, they risk compromising user trust and undermining their long-term sustainability. To address these concerns, it is essential to implement strict data protection regulations, such as GDPR, alongside mandatory compliance with ethical data governance practices by platform operators.

4.3 Case Study 3: Deceptive Practices in Zepeto

Zepeto, a metaverse platform operated by Naver Z, allows users to express multiple identities through avatars and interact within virtual worlds. However, the freedom of identity expression, which serves as a key advantage of the platform, has been exploited by some users for deceptive purposes.

As illustrated in Table 3 Deceptive Practices in Zepeto, certain users have created false identities to deceive others and manipulate trust. Reported incidents include the use of fake profiles or avatars to gain credibility, followed by attempts to engage in fraudulent financial transactions or extract personal information. Additionally, cases have emerged where false information was deliberately disseminated to incite social conflict for personal or ideological gain.

These deceptive practices have significantly eroded trust among Zepeto users, leading to a decline in the quality of social interactions within the platform. The exploitation of anonymity and identity fluidity in these cases starkly demonstrates the dual nature of multiple identities. Furthermore, these incidents reveal gaps in platform oversight mechanisms and the absence of robust ethical guidelines, underscoring the need for enhanced regulatory measures.

Table 3. *Privacy Violations in Horizon Worlds*

Case Overview	Platform	Zepeto (NAVER's Abartar-based Social Platform) *Naver: Korea's No.1 Portal
	Background	Some users create false identities to deceive others or incite social conflict.
	Major Stakeholders	Victims: Users who suffer economic or social harm due to misinformation. Perpetrators: Individuals who exploit false identities to undermine trust within the platform.
Ethical & Legal Problem Analysis	Problem Types	Deceptive Practices: Manipulating trust or spreading false information through fraudulent avatars.
	Cause of the Problem	Potential for False Identity Creation based on anonymity. Lack of a robust user verification system on the platform.
	Platform Response & Legal Limitations	Zepeto provides a reporting feature, but its preventive measures against deceptive practices are insufficient.
Victims & Social Impacts	Victims'Experience: Psychological distress and financial losses. Social Ramification: Decline in trustworthiness of interactions within the platform.	
Proposed Improvements	Platform Improvements: Strengthening false identity reporting systems and implementing user authentication procedures. Legal and Regulatory Recommendations: Establishing legal sanctions for deceptive practices using false identities.	

The Zepeto case illustrates how the freedom of self-expression enabled by multiple identities can be exploited for malicious purposes. To prevent such misuse, it is essential to implement enhanced identity verification systems, establish mechanisms for detecting fraudulent identities, and introduce educational programs to promote ethical digital behavior. Furthermore, clear regulatory frameworks and legal measures against deceptive practices must be in place to create a trustworthy, metaverse environment.

4.4 Case 4: The Patel Incident and the Issue of Virtual Sexual Harassment

One of the most notorious instances of virtual sexual harassment in the metaverse occurred in the Patel incident, which took place on Horizon Worlds. This case demonstrates how users can experience psychological harm in non-physical virtual environments that closely resemble real-world experiences.

In November 2021, during the beta testing phase of Horizon Worlds, Nina Jane Patel was subjected to sexual harassment within 60 seconds of logging into the platform. Her avatar was surrounded and physically obstructed by male avatars, who engaged in aggressive and inappropriate behavior. Even after the incident, Patel continued to receive derogatory and mocking messages, exacerbating her distress. She later stated, "Virtual reality is designed in a way that blurs the distinction between reality and simulation. As a result, I experienced both psychological and physiological reactions indistinguishable from

real-world trauma."

This case highlights several critical issues:

- Anonymity and Identity Exploitation – Perpetrators concealed their digital identities and leveraged anonymity to engage in unethical behavior without accountability.
- Legal Gaps – Since the incident occurred in a non-physical environment, it did not meet the legal criteria for physical contact, making prosecution under existing laws challenging.
- Psychological Reality of Virtual Harassment – Although the harassment took place in a virtual setting, Patel's psychological trauma was comparable to real-world experiences, emphasizing the severity of virtual sexual harassment.

The Patel case underscores the dangers of unethical behavior in the metaverse and the urgent need for regulatory frameworks to address such risks. It also highlights the importance of establishing ethical standards and legal responses tailored to digital environments. Without effective legal measures and platform governance, users remain vulnerable to identity exploitation and virtual harassment, making regulatory intervention a pressing necessity.

- The Patel incident serves as a pivotal case demonstrating that non-physical actions within virtual environments can result in consequences comparable to real-world harm. This underscores the urgent need to expand legal definitions

and establish comprehensive regulatory frameworks within the metaverse. In particular, the case highlights the necessity of implementing identity management systems, reinforcing platform accountability, and instituting robust legal mechanisms to safeguard users.

Table 4. *The Patel Incident and the Issue of Virtual Sexual Harassment*

Case Overview	Platform	Horizon Worlds
	Background	Nina Jane Patel experienced sexual harassment from other users during the beta test.
	Major Stakeholders	Victim: Patel suffered psychological trauma following the incident. Perpetrators: Exploited anonymity to engage in unethical behavior. Platform Operators: Lacked immediate intervention and failed to provide adequate user protection.
Ethical& Legal Problem Analysis	Problem Types	Virtual Sexual Harassment: Despite the absence of physical contact, the psychological impact was comparable to real-world experiences.
	Cause of the Problem	Regulatory Gaps in Anonymity and Non-Physical Environments.
	Platform Response & Legal Limitations	Immediate blocking measures were implemented within the platform, but no legal consequences followed. Existing legal frameworks fail to adequately address non-physical sexual harassment in virtual spaces.
Victims & Social Impacts	Victim's Experience: Severe psychological and emotional trauma. Social Ramifications: Raised concerns over metaverse safety and intensified ethical debates.	
Proposed Improvements	Platform Improvements: Strengthening anti-harassment features (e.g., safe distance settings, real-time monitoring). Legal and Regulatory Recommendations: Establishing clear legal definitions to criminalize non-physical sexual harassment in virtual environments.	

5. Discussion

5.1 The Dual Nature of Multiple Identities in the Metaverse

The formation of multiple identities in the metaverse carries significant positive implications, particularly in terms of expanding individual freedom of self-expression and enabling novel forms of social experience. Within these immersive digital environments, users can transcend physical limitations and explore diverse aspects of the self, enriching their social interactions through a variety of identity performances. Turkle (1995) argued that such multiplicity of identity allows individuals to derive psychological satisfaction and engage in meaningful self-exploration. On platforms like Zepeto, for example, users enhance their sense of social presence and interaction by creating and engaging through uniquely crafted avatars, which in turn fosters new forms of interpersonal connection.

However, the very freedom and fluidity that characterize multiple identities in the metaverse can also give rise to profound ethical challenges, particularly due to the anonymity and volatility of digital personas. A notable case on Roblox involved identity theft, where a perpetrator exploited a fabricated identity to build trust with underage users before committing financial fraud. This incident illustrates how the abuse of multiple identities can undermine trust-based social interactions and inflict real-world consequences that extend beyond the digital space.

Further examples, such as Horizon Worlds and the Patel case, demonstrate that multiple identities can facilitate unethical behavior of a severe nature. In these cases, perpetrators used anonymous digital identities to commit acts of virtual sexual harassment, while victims experienced psychological trauma comparable to that caused by physical offenses. These incidents underscore the urgent need to recognize that actions committed in non-physical environments may warrant the same ethical and legal scrutiny as those in physical spaces.

Thus, multiple identities in the metaverse are inherently dual in nature. While they offer valuable opportunities for self-expression and personal exploration, they also present considerable risks of ethical misuse and social harm. Platform design and legal governance must account for this duality, striving to establish a nuanced balance between user autonomy and the preservation of social trust.

5.2 Ethical Conflicts and the Necessity of Legal Regulation: Case-Based Analysis

The case studies examined in this research clearly demonstrate that the emergence of multiple identities in the metaverse can lead to significant ethical dilemmas and legal disputes. In the Roblox case, identity theft targeted minors and resulted in financial harm, illustrating how the absence of robust identity verification and management systems in virtual environments creates ample opportunities for abuse. When identities—ostensibly

built on trust—are fabricated, both social relationships and economic transactions can suffer severe consequences.

The Horizon Worlds case underscores deficiencies in data protection and consent mechanisms. The platform operator was found to have collected users' behavioral data and conversation logs without explicit consent, using them for commercial purposes. This constitutes a serious breach of user privacy and highlights the legal vacuum surrounding personal data protection in digital environments.

In the case of Zepeto, deceptive behaviors rooted in false identity construction reveal how multiple identities, when misused, can degrade social trust and disrupt the quality of user interactions on the platform. When users employ fictitious personas to manipulate others, the stability of social relations within the metaverse is compromised, thereby undermining the platform's integrity.

Perhaps most concerning is the Patel case, which brings attention to the severity of virtual sexual harassment within non-physical spaces. The perpetrator exploited anonymity and digital identity to inflict psychological trauma upon the victim. Yet, due to the limitations of existing legal frameworks—largely grounded in physical-world definitions of harm—no legal accountability was enforced. This case starkly illustrates the inadequacy

of traditional legal systems in addressing unethical conduct in virtual environments.

Collectively, these cases illustrate that ethical conflicts in the metaverse manifest predominantly in four domains: identity-based fraud, data privacy violations, trust-oriented deception, and non-physical forms of violence. Each category poses unique challenges to both platform governance and legislative systems, thereby necessitating urgent and targeted regulatory responses.

5.3 Limitations of Existing Legal Frameworks and Multi-Stakeholder Regulatory Directions

While the metaverse enables the free experimentation of multiple identities and fosters new modes of social interaction, existing legal frameworks are structurally inadequate to govern the complex ethical and legal challenges that arise in such environments. Issues such as identity theft, privacy breaches, the misuse of anonymity, and jurisdictional ambiguity are further exacerbated by the metaverse's unique technological architecture and its inherently transnational nature. Addressing these problems requires a clearly delineated set of responsibilities across stakeholders, accompanied by comprehensive legislative reform.

First, Strengthening Platform Responsibility for Identity Verification and Ethical Governance: Platform providers must implement identity registration and verification

systems to facilitate trust-based interactions among users. While maintaining the principle of anonymity, platforms should adopt a limited real-name policy—such as internally linked identifiers based on verified credentials—that ensures accountability in the event of misconduct. In the context of Korean law, Article 17 of the Personal Information Protection Act could be amended to explicitly categorize behavioral data and avatar activity logs as personal information. This would legally mandate data retention and traceability in the event of violations. Moreover, platforms should introduce real-time reporting mechanisms, digital ethics guidelines, and educational content to simultaneously uphold user autonomy and platform safety.

Second, Establishing Governmental Mechanisms for Data Protection and Digital Citizenship: Governments must develop standards to enhance transparency in data use and privacy protection, and reflect these in national legislation. This includes detailing the collection, use, storage, and deletion processes for sensitive data such as user conversations, behavioral patterns, and location information. A robust enforcement structure should also be created to sanction the misuse of personal data. Specifically, amendments to the Personal Information Protection Act should introduce a new chapter on metaverse-specific data protection, harmonized with global standards such as the GDPR. Furthermore, a new Digital Citizenship Protection Act should be considered to protect

users from identity theft, virtual violence, and similar harms. This legislation would serve as a comprehensive legal basis for defining the rights, responsibilities, and safety standards of citizens in metaverse environments.

Third, Expanding Legal Definitions of Non-Physical Harm in Legislative Bodies: Current laws such as Article 298 of the Criminal Act (sexual assault) and Article 44-7 of the Information and Communications Network Act are predicated on physical acts occurring in physical spaces. As a result, they are ill-equipped to address virtual forms of harm—such as sexual harassment, hate speech, and deception—that occur within the metaverse. The Patel case underscores this limitation, where the victim suffered serious psychological trauma, yet the existing legal provisions failed to hold the perpetrator accountable. Article 298 should be amended to explicitly include "sexual acts via avatars in virtual environments," and Article 44-7 should incorporate provisions related to "non-physical harmful expressions in digital settings." Such revisions would legally recognize psychological and social harm that occur in non-physical environments as prosecutable offenses.

Fourth, Resolving Jurisdictional Ambiguities through International Cooperation and Standardization: Given the cross-border nature of the metaverse, national laws alone are

insufficient to resolve criminal or civil disputes. Jurisdictional conflicts are especially problematic when the location of the crime, the nationality of the offender, and the platform's headquarters are all situated in different countries. To mitigate such challenges, international organizations such as the OECD and the United Nations should spearhead a Global Metaverse Ethics and Legal Accord. Provisions related to the metaverse could be appended to existing instruments such as the Budapest Convention on Cybercrime, forming the basis for international legal cooperation in digital environments. Such global efforts would help clarify responsibilities for both users and platforms, and compel multinational platforms to adhere to a baseline of ethical and regulatory standards.

6. Conclusion

6.1 Summary of Findings and Key Implications

This study examined the multifaceted impacts of multiple identities in the metaverse on user experience and social interaction, while critically analyzing the accompanying ethical dilemmas and legal challenges. The metaverse offers a unique digital environment in which users can transcend physical limitations to explore diverse aspects of selfhood and cultivate novel social relationships. However, this same environment also fosters significant risks, including identity theft, privacy violations, deceptive behaviors, and virtual sexual harassment.

The case study of Roblox illustrated how trust-based interactions can collapse when virtual identities are exploited to inflict economic harm on minors. The Horizon Worlds case revealed critical legal voids surrounding data privacy, as user behavioral information was collected and utilized without consent. On Zepeto, instances of deceptive identity fabrication undermined interpersonal trust within the platform. Furthermore, the Patel case demonstrated that anonymity and digital identity can be misused to commit acts of virtual sexual harassment, leading to psychological trauma akin to that experienced in the physical world.

These findings underscore the dual nature of multiple identities in the metaverse. On the one hand, they serve as instruments of personal expression and catalysts for enriched social interaction. On the other hand, they may be exploited in ways that magnify ethical conflicts and legal ambiguities, particularly when amplified by platform anonymity and technological loopholes.

This study therefore emphasizes that recognizing and managing this duality is essential. It concludes that building a sustainable and trustworthy metaverse ecosystem requires the delineation of clear ethical and legal responsibilities across all key stakeholders—including platforms, governments, legislatures, and users. Such multi-actor

coordination forms the foundation for ensuring both freedom of identity exploration and the protection of individuals from harm within immersive digital environments.

6.2 Policy and Legal Recommendations

To address the ethical conflicts and legal challenges emerging in the metaverse while preserving the social and cultural value of multiple identities, this study proposes a set of stakeholder-specific policy and legal measures. The primary objective is to clearly delineate the roles and responsibilities of platforms, governments, legislative bodies, users, content creators, and international organizations, and to revise relevant laws and ethical standards in order to foster a safer and more sustainable metaverse ecosystem.

First, strengthening identity management and ethical accountability of platform operators. Platform providers must implement technology-based systems for identity registration and avatar authentication to prevent impersonation and ensure trust-based interactions. While preserving a degree of anonymity, a limited real-name verification system—such as internally linked identifiers based on real-name authentication—should be introduced to enable accountability in the event of unlawful conduct. Article 17 of Korea's Personal Information Protection Act should be revised to explicitly define avatar behavioral data as personal information, thereby enabling the retention and use of such logs as legal evidence in case of misconduct. Additionally, platforms must assume

responsibility for cultivating ethical usage cultures by offering real-time reporting functions, ethical guidelines, and user education programs. They should also establish internal surveillance systems and user protection infrastructures.

Second, institutionalizing government-led data protection and digital citizenship. Governments should introduce metaverse-specific provisions into the Personal Information Protection Act to regulate the collection and use of sensitive data such as conversations, behavior patterns, and location data. These regulations must align with international standards such as the GDPR and include explicit protocols for consent, data storage, and deletion. Moreover, the enactment of a "Digital Citizenship Protection Act" is necessary to define and penalize offenses such as identity theft, virtual violence, and emotional harm. Such legislation could serve as a charter safeguarding civil rights and responsibilities in virtual environments.

Third, expanding legal definitions of non-physical harmful acts. Current laws such as Article 298 of the Criminal Act (sexual assault) and Article 44-7 of the Information and Communications Network Act are grounded in physical reality and thus insufficient for addressing virtual misconduct such as avatar-based harassment, deception, and hate speech. These statutes should be explicitly amended to include non-physical acts such as

"sexual conduct via avatars in virtual environments" and "psychological harm in digital contexts," thereby extending legal protections to intangible forms of victimization.

Fourth, reinforcing the ethical responsibility of users and content creators. Users should be required to sign a digital ethics pledge or complete a basic ethics training program upon joining metaverse services, thereby internalizing the community's normative values. Content creators must adhere to self-regulatory principles regarding youth protection, prohibition of hate speech, and age-appropriate content. They also have a responsibility to lead responsible creative practices based on jointly established ethical guidelines among governments, platforms, and industry stakeholders.

Fifth, establishing international cooperation and global regulatory standards. Given the transnational nature of the metaverse, it is imperative to establish a global legal framework through international bodies such as the OECD and UN. This includes signing a "Metaverse Ethics and Legal Convention" and incorporating metaverse-specific provisions into existing cybercrime treaties. A cooperative legal mechanism among nations must be developed to resolve jurisdictional conflicts and impose mandatory ethical and data protection standards on global platform operators.

These multi-actor policy and legal recommendations aim to protect the constructive

potential of multiple identities in the metaverse while minimizing ethical risks and legal liabilities. They offer a practical and implementable framework for building a trustworthy digital society and ensuring responsible innovation in immersive virtual environments.

6.3 Limitations and Directions for Future Research

While this study has examined the issue of multiple identities within the metaverse through detailed case analysis, several limitations remain.

First, the research lacks empirical data on user experience due to its case-centered methodology. Although ethical and legal issues were highlighted through the analysis of incidents such as those on Roblox, Horizon Worlds, Zepeto, and the Patel case, qualitative and quantitative data—such as user interviews or surveys—were not collected. Future research should incorporate empirical user data to investigate how multiple identities are actually perceived and experienced in metaverse environments.

Second, the study does not fully reflect the technical and ecological differences across various metaverse platforms. Metaverse platforms differ significantly in their architectural design, community governance, and content creation mechanisms. These differences may influence how multiple identities function and how ethical dilemmas manifest. Comparative analyses across platforms are therefore needed to generate more

tailored policy and regulatory recommendations.

Third, the legal frameworks analyzed in this study primarily focus on South Korea, the United States, and the European Union. This limits the generalizability of findings to the broader global metaverse context. Future studies should include legal perspectives from other regions, such as Asia, Latin America, and the Middle East, to examine disparities in regulatory readiness and the feasibility of international harmonization. Research into the mechanisms for legal alignment and consensus-building across jurisdictions will be especially important for the development of shared global norms.

Fourth, the rapid evolution of metaverse technologies poses a challenge to the temporal relevance of research findings. Static regulatory recommendations may become outdated as technologies and societal dynamics shift. Therefore, continuous exploration of adaptive legal frameworks that account for the dynamic interaction between technological advances and social values is essential.

Finally, while this study proposes stakeholder-specific legal and ethical responsibilities, it does not empirically examine how these actors—platform operators, government regulators, users, and content creators—actually perceive, internalize, or implement these responsibilities. Future research should assess the accountability

mechanisms and behavioral responses of each stakeholder group to validate the effectiveness of proposed interventions.

Future studies may further explore AI-based regulatory frameworks, ethical education systems for metaverse users, and the practical viability of identity management technologies. These extensions will help establish a safer and more inclusive digital ecosystem in which multiple identities can support self-exploration and social cohesion in the evolving landscape of the metaverse.

Funding: This work was supported in part by the MSIT(Ministry of Science and ICT), Korea, under the Graduate School of Metaverse Convergence support program (RS-2022-00156318) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

References

Kim, E. Y. (2022, Nov. 16). Customers in the Metaverse Era. *ChosunBiz*. https://biz.chosun.com/distribution/channel/2022/11/13/JQTBC6OPZRAPLJCUQRIL5VDL2U/

Lee, Y. R. (2023). The legal status of metaverse avatars: Focusing on the recognition of personhood. *Seoul Law Review*, *31*(2), 1-38.

Jang, C. R & Lee, S. Y. (2024). An exploratory study on the effects of Zepeto users' avatar types, social presence, and self-presence on flow experience. *Korean Journal of Broadcasting and Telecommunication Studies*, *38*(1).

Heo, J. E. & Nam, J. E. (2023). A qualitative case study on the multiple identities of adolescent metaverse Creators. *Youth Culture Forum*, *75*.

Vigderman, A., & Turner, G. (2025, Mar. 21). IS Roblox Safe? *Security*. https://www.security.org/digital-safety/is-roblox-safe/

Banks, J. (2015). Object, Me, Symbiote, Other: A social typology of player-avatar relationships. *First Monday*, *20*(2).

Daniel E., & Istvan, Z. (2016). Identity theft in the virtual world: Analysis of a copyright crime in Second Life from the perspective of criminal law and IT forensics. *HJLS*, *57*(4), 489-509.

de Zwart, M. J., & Lindsay, D. F. (2012). My self, my avatar, my rights? Avatar identity in social virtual worlds. In D. Riha (Ed.), *Frontiers of Cyberspace* (1st ed., pp. 81 - 100). Rodopi.

Diana Clement (2022, Jun. 2). The Law Association of New Zealand, Sex in the metaverse: virtual body, real sexual assault. *The Law Association*. https://thelawassociation.nz/sex-in-the-metaverse-virtual-body-real-sexual-assault/

Donath, J. (1999). Identity and deception in the virtual community. In M. A. Smith & P. Kollock (Eds.), Communities in cyberspace (pp. 29-59). Routledge.

Emory Law Journal. (2020). Hey, you stole my avartar!: Virtual reality and its risks to identity protection. *Emory Law Journal*, *69*, 833-878

Lin, J., & Latoschik, M. E. (2022). Digital body, identity and privacy in social virtual reality: A systemic review. *Front, Virtual Real*, *3*.

Jon, G. (2008). Playing in the virtual arena: Avatars, publicity, and identity reconceptualized through virtual worlds and computer games. *Chapman Law Review*, *11*(3).

Klimmt, H., & Vorderer, P. (2009). The video game experience as 'true' identification: A theory of enjoyable alterations of players' self-perception. *Communication Theory*, *19*(4), 351–373.

Naseh, M. V. (2016). Person and personality in cyberspace: A legal analysis of virtual identity. *Masaryk University Journal of Law and Technology*, *10*(1), 1-22.

Parmentier, G. & Rolland, S. (2009). Consumers in virtual reality: Identity building and consuming experience in Second Life. *Recherche et Applications en Marketing (English Edition)*, *24*(3), 43-55.

Turkle, S. (1995). Constructions and reconstructions of self in virtual reality: Playing in the

MUDs. *Mind, Culture, and Activity*, *2*(3), 158-167.

Turkle, S. (2003). *Life on the Screen (Translated by Choi Yu-sik)*. Seoul: Minumsa (1995).

van Kokswijk, J. (2007). Legal aspects of virtual identity. *proceedings of the international conference on cyberworlds*, 77-81.

Walbesser, J. L. (2014). Finding meaning in the death of virtual identities. *Buffalo Intellectual Property Law Journal*, *10*, 70-91

Wearing, M. (2011). *Social Identity*.

Yaqoub Alsarkal, Nan Zhang, & Yilu Zhou. (2015). *Linking virtual and real-world identities*. IEEE.

Appendix

1. Analytical Framework for Case Study Analysis

1.1 Case Overview

1.1.1 Background of the Incident

- Characteristics and primary activity environment of the metaverse platform where the incident occurred (e.g., Roblox, Horizon Worlds, Zepeto, etc.).
- Timeline and contextual background of the incident.
- Key aspects of multiple identities involved in the case (e.g., anonymity, identity switching).

1.1.2 Key Stakeholders

- Victim: Age, gender, type of activities, and engagement within the platform.
- Perpetrator: Identity characteristics (e.g., level of anonymity, behavioral motives).
- Platform Operator: Role and responsibility of the metaverse platform regarding the incident.

1.2 Ethical and Legal Issues Analysis

1.2.1 Types of Issues

- Identity Theft: Unauthorized impersonation and misuse of virtual avatars or identities.
- Privacy Violations: Data breaches, unauthorized data collection, and exploitation.
- Deceptive Practices: Fraudulent identity creation and abuse of trust.
- Other Ethical Concerns: Virtual sexual harassment, unethical behaviors leveraging anonymity.

1.2.2 Root Causes of the Issues

- Platform Design Flaws (e.g., absence of identity verification mechanisms, inadequate reporting procedures).
- Ethical Limitations in User Behavior (e.g., identity exploitation, malicious activities).
- Deficiencies in the Existing Legal Framework (e.g., gaps in legal provisions addressing virtual identity-related misconduct).

1.3 Platform and Legal Responses

1.3.1 Initial Response by the Platform

- Immediate actions taken by platform operators following the incident (e.g., handling of reports, user bans).
- Assessment of the effectiveness of platform policies and regulatory systems.

1.3.2 Legal Intervention

- Application of relevant laws (issues related to jurisdiction, applicable legal provisions).
- Legal outcomes (protection of victims, penalties imposed on perpetrators).
- Limitations of the legal framework (e.g., lack of legal definitions for non-physical offenses, jurisdictional conflicts).

1.4 Impact on Victims and Society

1.4.1 Victim's Experience and Consequences

- Psychological and social impact on the victim (e.g., trauma, economic loss).
- Perceived lack of protection from platform policies and legal systems.

1.4.2 Social Implications

- Erosion of trust within the platform's user community.
- Ethical debates in media and public discourse, highlighting the responsibility of virtual spaces and the need for regulation.

1.5 Recommendations for Improvement

1.5.1 Platform-Level Improvements

- Implementation of identity verification and registration systems.
- Strengthening privacy protection and data management policies.
- Enhancing user reporting mechanisms and dispute resolution procedures.

1.5.2 Legal-Level Improvements

- Establishing legal definitions and penalty standards for different types of incidents.
- Developing an institutional framework for international cooperation and jurisdictional resolution.

1.5.3 User Education and Ethical Reinforcement

- Implementing educational programs to prevent identity misuse and exploitation.
- Establishing and promoting ethical behavioral guidelines for virtual environments.

1.6 Conclusion

- Summary of key lessons and implications derived from the case study.
- Emphasis on the importance of ethical and legal governance in managing multiple identities in the metaverse.
- Contribution to preventing similar incidents and fostering a sustainable metaverse ecosystem.