

Shin, Sunkyung; Park, Joo-Yeun

Conference Paper

A Study on Metaverse Risks and Risk Perceptions

24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Shin, Sunkyung; Park, Joo-Yeun (2024) : A Study on Metaverse Risks and Risk Perceptions, 24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024, International Telecommunications Society (ITS), Calgary

This Version is available at:

<https://hdl.handle.net/10419/302464>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

A Study on Metaverse Risks and Risk Perceptions

Sunkyung Shin

Research fellow, Institute of Media Communication,

Hankuk University of Foreign Studies

Joo-Yeun Park

Professor, Hankuk University of Foreign Studies

Keywords: Metaverse, Extended reality, Virtual environments, Digital Risk

1. Introduction

The development of Metaverse technology is transforming our lives by shifting our daily activities from the offline to the online world. Metaverse has begun to be recognized as a key industry and future technology by leading the onlineization of daily life that is impossible in reality due to the disaster situation of COVID-19.

Metaverse, which is based on the meaning of the expansion and extension of the physical world to the virtual world, is opening a new chapter in human communication and is recognized as a space with new possibilities (Lee et al., 2021). However, the new opportunities and possibilities offered by Metaverse are accompanied by both the positive functions and effects that were expected and targeted in the development and introduction of early metaverse, as well as the unintended negative functions and effects (Dwivedi et al., 2023). In other words, from a future perspective, Metaverse is a revolutionary technology that will change our living environment, and it is quickly permeating our daily lives more than any other technology, but the side effects associated with it are also quickly expanding their influence into our lives.

As the industrial importance of the Metaverse has increased, Metaverse technology has been applied to various fields, and new

services and platforms based on the Metaverse have emerged, and the number of users has also increased rapidly (Barrera & Shah, 2023). As a result of this situation, the influence of the Metaverse has expanded beyond the industrial dimension to social influence such as individuals and society. In particular, the innovative characteristics of the Metaverse, which are different from existing technologies, have allowed users to experience new side effects that they have never experienced before, and have even expanded to the form of social conflict. These side effects of using the Metaverse are presented as a new challenge and task that must be overcome for the development and future of the Metaverse industry.

In response to this situation, this study starts from a critical perspective on the fact that previous studies on Metaverse technology and services have focused too much on the technical aspects and have been discussed only from an optimistic point of view (Bogicevic et al., 2021; Book, 2004; Flavián et al., 2019). In particular, just as all digital media technologies and services have a double-edged sword, the Metaverse also has a double-edged sword, and behind its positive effects lie the risks of negative effects. In this study, we aim to identify and address the risks and threats inherent in Metaverse technologies and services, and to specify and categorize the risks

that arise from the use of Metaverse technologies and services, in the context of extending digital risk research and initiating Metaverse risk research. In addition, this study aims to conduct an empirical study on the experiences and perceptions of users who actually use Metaverse technologies and services regarding the risks associated with the use of Metaverse technologies and services.

Therefore, this study, considering the situation that instability exists due to the spread and use of the Metaverse, but sufficient discussion has not been made on this, intends to discuss the Metaverse risk from a comprehensive perspective for the stable use and spread of the Metaverse. Starting with this, we aim to establish a theoretical foundation that can continue to expand Metaverse research in the future.

2. Understanding the evolution of the Metaverse

2.1. Overview of the Metaverse Industry

The Metaverse is a combination of the prefix “meta” meaning “transcendence” and the word “universe”, and refers to a simulation environment that combines physical reality and virtual reality (Ball, 2022). However, the term Metaverse is not a recent concept, and was first mentioned in the 1992 novel <Snow Crash> by Neal Stephenson, meaning a virtual universe, an evolutionary concept of the virtual world (Stephenson, 1992).

However, the Metaverse as we know it today is a more advanced concept than traditional virtual worlds, possessing a more complex structure. Consequently, researchers and organizations offer varying definitions of the Metaverse, and its precise definition remains elusive despite its commercialization (Cho & Moon, 2023). Particularly within the contemporary media ecology, the Metaverse presents a definitional challenge due to its genesis through the synergistic convergence of

technologies, services, and broader technological evolution, mirroring the emergence of other smart media offerings. Despite these definitional challenges, the Metaverse's burgeoning industrial applications have propelled its growth potential to new heights, gradually diminishing the ambiguity surrounding its concept. When defining the Metaverse, a common perspective emerges: it possesses distinct technological and environmental characteristics that set it apart from existing media services and platforms (Bobier et al., 2022; Lee et al., 2021). In light of this discussion, this study defines the Metaverse we currently utilize as a platform where a second self, an avatar, acts beyond physical space based on technologies such as virtual reality, augmented reality, and mixed reality.

As evident in the definition of the Metaverse concept, it is employed in a more advanced sense than traditional virtual worlds. Accordingly, virtual world types within the Metaverse environment are being categorized in greater detail. Specifically, Bell et al. (2004) classify virtual worlds into immersive, non-immersive, and augmented virtual worlds in their study of detailed type differentiation.

Immersive virtual worlds, as defined by Castronova (2003) and Jackson et al. (2007), share same concept as the game-type virtual world classified, but it has the characteristic of being a simulation provided in a fictional space. Notable examples of immersive virtual world services include: NCsoft's <Lineage>, Blizzard Entertainment's <World of Warcraft (WOW)>, and Riot Games' <League of Legends (LoL)>.

Non-immersive virtual worlds, as defined by Castronova (2003) and Jackson et al. (2007) are also referred to as “networked virtual worlds” or “life-like virtual worlds”. These virtual worlds are based on everyday and social functions, allowing users to expand their activity range beyond their physical space into a virtual realm where they can establish new communication spaces and social networks.

The last type is the augmented virtual

world. This world build upon traditional virtual world by incorporating users' diverse purposes into their services. In essence, augmented virtual worlds represent a convergence of immersive and non-immersive virtual worlds. As a result, augmented virtual worlds can be considered hybrid platforms that combine the immersive aspects of gaming and social interaction with the life-like features of non-immersive virtual worlds, allowing users to enjoy games and engage in social activities with other users. In other words, due to recent media technology and environmental evolution, services that previously functioned as game-type or life-type virtual world platforms are being reorganized into augmented virtual world platforms by adding life and communication functions or game functions. As a result of this convergence, several Metaverse platforms have emerged, including: Roblox Corporation's <Roblox>, NAVER Z's <ZEPETO>, and SKT's <ifland>. In short, technological advancements have paved the way for the emergence of diverse Metaverse platforms, each with its unique characteristics and functionalities. The COVID-19 pandemic further accelerated the adoption of these platforms, particularly those with multifaceted capabilities. As a result, the Metaverse landscape has evolved, with hybrid Metaverse platforms like <Roblox>, <ZEPETO>, and <ifland> taking center stage in today's industry.

2.2. Understanding Two Perspectives on the Metaverse

2.2.1. The Metaverse as a Transformative Technological Paradigm

The value of the Metaverse is well demonstrated in the diversity of Metaverse technology and service utilization. In our society today, Metaverse technology is rapidly expanding beyond the boundaries of the original media content industry such as culture, art, and entertainment to various fields such as education, marketing, production and manufacturing, and

finance, thereby increasing its value (Wang et al., 2023).

In fact, global luxury brands such as Gucci and Balenciaga have launched digital fashion NFT (non-fungible tokens) that users can purchase through their avatars via the Metaverse platform. In addition, these digital fashions are sold in the same way in real stores, realizing digital twins (Bale et al, 2022). US President Biden is also famous as a representative politician who actively utilizes the Metaverse. During the 2020 presidential election, when it became difficult to hold large-scale rallies due to the COVID-19, President Biden conducted his election campaign through the Metaverse. In the wake of COVID-19, a transformative influence has been exerted on both the political sector and the entertainment industry paradigm. A paradigm case of a large-scale gathering held through the Metaverse is the concert by American rapper Travis Scott. Travis Scott hosted a concert via <Fortnite>, an American Metaverse platform, in April 2020. This event stands as a paradigm case of a large-scale gathering that mitigated the constraints imposed by COVID-19, recording more than 12.3 million concurrent attendees (Oh, 2021). While concerts and other cultural events have long been held in the Metaverse, the scope of virtual gatherings is rapidly expanding. Recent examples include graduation ceremonies, freshman orientation events, and even corporate presentations. This trend highlights the Metaverse's potential to transcend its role as a mere extension of social media and evolve into a next-generation platform with global reach. As such, the potential applications and expansion of the Metaverse within our society are expected to be limitless.

2.2.2. Side Effects and Risks: Associated with Metaverse Usage

The convergence of digital and communication technologies with the Metaverse is revolutionizing the media landscape, making it smarter and more responsive than ever before. The

rapid growth and widespread adoption of the Metaverse are accelerating the transition from an offline-centric lifestyle to an online-centric one. This shift is fundamentally altering how we interact, engage, and experience the world around us. While technological advancements bring about undeniable benefits, it is crucial to acknowledge the inherent duality of technology, often referred to as "Technological Dualism." This concept emphasizes that every technology, including the Metaverse, possesses both positive and negative aspects that must be carefully considered. According to Lupton (2016), as innovative media technologies such as digital media, smart devices, and software are rapidly applied to our lives, various problems are occurring around them. In addition, McQuail (1983) emphasizes that due to the duality of technology, problems that arise from the use and diffusion of new technologies and services are not limited to problems at the individual level, but are expanded to social and collective impacts. In this way, the Metaverse has both positive and negative effects. In the case of side effects resulting from the use and spread of innovative digital technologies and services such as the Metaverse, there are still unpredictable risks that have not been revealed yet, but are still partially revealed, in the complexly intertwined relationships between society, technology, and users.

As the risks occurring in the Metaverse are recognized as social issues rather than personal ones, research on Metaverse-related risks is being conducted. However, in the case of Metaverse risk studies conducted so far, similar to the early studies on cybercrime, they are mainly conducted by individually analyzing the crime phenomena occurring or listing the types of occurrence.

The risks associated with Metaverse usage can be broadly categorized into three types: individual risks, societal risks, and economic risks (see [Table 1]).

Table 1
Classification of Metaverse Risk

Risk factors	Definition	Reference
--------------	------------	-----------

Individual risks	Personal	Types of risks triggered by individual choices that are related to personal safety and life	Cho (2011), Hong (2005)
	Physical-health	Types of physical and health risks that can occur to users depending on their use of the Metaverse platform	
	Societal Risks	Types of risks that may become social problems due to the use of Metaverse	
	Economic Risks	Types of economic risks that users may encounter significant financial and investment challenges	

Individual risks refer to the direct threats faced by Metaverse users. These risks can manifest in various forms, including: Privacy, Cyberbullying and Harassment, Data sovereignty infringement, Surveillance society, Addiction and obsessive behavior, Physical Health Concerns, Mental Health Concerns (Ban & Nam, 2023; Ryu, 2022; Hwang, 2023). Individual risks can be further categorized based on the target and characteristics of the risk. These categories are Personal risks and physical health risks (Cho, 2011). Personal risks are general-level risks related to the user's daily life. Individual risks in the Metaverse, particularly those related to cyberbullying, represent an extension of existing cyberbullying threats into the immersive and interactive virtual environment. As in traditional cyberbullying, these risks involve the intentional use of digital technologies, such as avatars, virtual chat, and social media platforms, to harm or harass others within the Metaverse. That is, in the case of individual risks occurring in the Metaverse environment, it was recognized as cyber violence in the past, and it is an act that violates the autonomy or personal rights of others in cyberspace, and it is mainly characterized by occurring through information and communication technologies such as digital devices (Kim, 2022). However, in the case of individual risks occurring in the recent Metaverse platform, which is an evolved cyberspace, it is becoming more

sophisticated than existing risks. In addition, in the Metaverse environment, in addition to traditional sexual violence crime types such as stalking and sexual harassment, more evolved crime patterns are appearing in connection with innovative technologies such as AI (Artificial Intelligence).

Physical-health risks, on the other hand, are specific to individuals and have a pathological nature. These risks can be further categorized into addiction and obsessive behavior, physical health concerns, and mental health concerns. Unlike individual risks that occur in the virtual world, the consequences of such harm extend to the real world (National Information Society Agency, 2020.12.).

Societal risks are those that impact the overall structure and systems of society. In the context of the Metaverse, societal risks arise from the use of Metaverse technologies and services. These risks extend beyond individual users and can affect society as a whole, potentially leading to crises in social functioning and even the survival of society itself. So it is important to be aware of the potential societal risks associated with the Metaverse. These risks can be broadly categorized into the following areas: Information overload, Malicious code and viruses, Illegal and harmful information, Hacking, Digital divide, Internet trolls, Sudden service malfunctions and interruptions, Conflicts between regulation and freedom of expression, Job displacement, Language destruction, Infodemics, Cyber gambling (Choung, 2022; Lee, 2022). In the case of societal risks occurring in the Metaverse environment, not only are problems already pointed out as problems in the existing digital media usage environment, but new problems are also occurring in areas that were not previously recognized as problems or, in particular, did not occur.

The Metaverse has emerged as a transformative force, creating a unique economic ecosystem that seamlessly integrates virtual and real-world economies. This convergence has opened up a plethora of opportunities for

businesses and individuals to engage in diverse economic activities within the Metaverse's immersive environment. While the Metaverse presents a captivating realm of economic possibilities, its burgeoning virtual economy is not without its perils. The very factors that drive its growth also harbor the potential for unforeseen economic drawbacks, casting a shadow over the future of the Metaverse industry and its technological underpinnings. The economic risks associated with the Metaverse extend beyond mere inconveniences or financial setbacks (Katterbauer et al., 2022). They represent a significant threat to the stability of the economic environment and the well-being of individuals. These economic risks can be broadly categorized into the following areas: Financial scams and fraud issues and Intellectual Property and Copyright (Bhardwaj, 2024; Shafik, 2024).

In summary, the results of previous studies show that the Metaverse, an agglomeration of ICT, is quickly settling into our society, but it is also showing various side effects. In particular, the risks currently observed on the Metaverse platform are comprehensive and complex, including not only existing risks but also new risks that have not been experienced before. The comprehensive digital risk factors occurring in the Metaverse environment, which were organized by referring to these previous research results, are as shown in [Table 2]. What can be confirmed through [Table 2] is that the risks occurring in the current Metaverse environment are the same as existing risks, but their status and degree have evolved compared to existing risks, and not only that, they are becoming more complex beyond existing digital risks to new types of risks.

Table 2
Metaverse Risk Factors and Definitions

Risk factors	Definition	Reference
Individual Risks		
Privacy	The unauthorized disclosure of personal information, such as the name, gender, address, and phone number of Metaverse platform users, to others without their	Hur (2010)

	consent, which constitutes a violation of their right to self-determination of personal information		bypassing information and communication networks	
Cyberbullying and Harassment	Unmoral behavior in which an avatar controlled by a user attempts verbal or sexual assault on an avatar controlled by another user, causing physical and mental harm	Park (2022)	Digital divide	Relative deprivation experienced by users of Metaverse platforms compared to non-users, including knowledge and information gaps, communication and social participation gaps Kang (2022)
Data sovereignty infringement	The act of platforms collecting, datafying, and utilizing information about individuals, resulting in the loss of information subjects' opportunities and abilities to utilize their own information	Yun (2013)	Internet trolls	The act of inciting negative emotions in other users by sharing inflammatory and offensive content or writing comments within Metaverse platforms Molenda et al. (2022)
Surveillance society	The act of monitoring, recording, classifying, and controlling the activities and overall environment of users within the Metaverse environment by a specific individual or government	Cho & Kim (2016)	Sudden service malfunctions and interruptions	Errors experienced by users at the time of service use due to the failure to meet planned technical criteria Ahn et al. (2022)
Addiction and obsessive behavior	The pathological phenomenon of excessive Metaverse platform usage that disrupts daily life		Conflicts between regulation and freedom of expression	The conflict between the right to control personal information (self-information management control right), which allows the data subject to judge, refuse, and control the processing of information, and the right to know, which is the freedom of expression Cho & Kim (2016)
Physical Health Concerns	Physical harm to users caused by experiencing virtual reality platforms and devices, including dry eyes, vision loss, carpal tunnel syndrome, and cybermotion sickness	Lee (1999)	Job displacement	The changes in the work environment and employment centered on virtual space as various industries and businesses introduce Metaverse technology and services on-site Lee et al. (2016)
Mental Health Concerns	Mental harm to users caused by experiencing virtual reality platforms and devices, including anxiety, delusions, insomnia, and fatigue		Language destruction	The phenomenon of language variation through the use of 'new words,' 'vulgar language,' 'onomatopoeia,' and 'foreign words' in communication via online platforms Park et al. (2016)
Societal Risks			Infodemics	By the spread of distorted information through Metaverse platforms, leading to crises in individuals, society, and security Cho & Kim (2016)
Information overload	The gap between the amount of information generated by ICT advancements and the information processing capacity of users	So & Kim (2017)	Cyber gambling	Speculative behavior in the Metaverse environment through the use of cryptocurrency or digital finance transactions Choung (2007)
Malicious code and viruses	The unauthorized intrusion into another user's information and communication network constitutes a severe cybercrime that aims to disrupt system and Metaverse platform operations. This malicious activity involves employing Denial-of-Service (DoS) attacks and deploying malware to render systems and Metaverse platforms inoperable	Lee, W. S. (2022)	Economic Risks	
Illegal and harmful information	The distribution, display, or sale of content that violates sexual morality through information and communication networks	Yun & Yu (2012)	Financial scams and fraud	Deceiving other users in the Metaverse platform through false information during transactions involving virtual currencies and items Lee & Min (2021)
Hacking	Gaining unauthorized access to a user's system through abnormal means, such as disabling or	Cho & Kim (2016)	Intellectual Property and Copyright	Intellectual property infringement in the Metaverse refers to the violation of rights associated with original creations of the mind within Metaverse environments. These creations encompass literary and artistic works, designs, symbols, names, and

3. Metaverse Users' Risk Perception

The perception of risk can be categorized into objective and subjective risk, and these two cognitive concepts differ based on the interpreting subject. Firstly, objective risk perception refers to the evaluation of risk in an objective manner. This entails assessing the likelihood of a risk occurring using precise statistical methods such as probability from an expert's perspective. However, according to Slovic (1992), risk is inherently subjective due to the impossibility of measuring the exact and complete frequency of occurrence for specific risks and the inability to exclude the influence of social, environmental, and historical factors on risk perception when interpreting collected information and data.

In light of the limitations of objective risk perception and its measurement, the concept of 'subjective risk perception' has emerged, focusing on evaluating how actual users perceive risk (Kwon & Cha, 2021). Subjective risk perception involves individuals assessing risk based on their personal experiences, knowledge, and beliefs, and using this assessment to determine whether or not to adopt new technologies. The concept of subjective risk perception was introduced within the framework of the Health Belief Model in health communication. This means that individuals' perceptions of the probability and seriousness of natural or man-made risks that threaten their health, along with other personal cognitive assessment factors, influence their beliefs and actions related to these risks (Kim & Kim, 2007). While estimating the objective probability of risk occurrence can be challenging, subjective risk perception can be quantified by measuring users' perceived likelihood of risk occurrence using a scoring system. Similarly, the perceived seriousness of the consequences of risk occurrence can also be scored using a scale (Health & Safety Executive, 1998). Building on

this, the measurement of subjective risk perception is generally conducted by combining the perceived probability of risk occurrence and the perceived seriousness of the consequences (Risk Occurrence Perception \times Risk seriousness Perception) (Song & Kim, 2013).

As the media landscape has gradually shifted towards a user-centric approach, risk discussions from the perspective of users, the actual stakeholders, have become more prevalent. Currently, user risk assessment is recognized as more important than expert assessment, leading to a surge of user-centered risk research in various media studies, replacing the traditional expert-centric approach (Bale et al., 2022; Berger et al., 2018; Wei et al., 2019).

In summary, Metaverse platforms have emerged as a pivotal force not only in the media industry but across society, driven by both the benefits offered by technology in the era of innovation and services and the unique social and environmental impact of the COVID-19. However, the benefits that Metaverse technologies and services provide to our society are accompanied by potential drawbacks and risks stemming from the inherent duality of technology. Therefore, multifaceted discussions based on diverse perspectives are essential for the sustainable development of Metaverse technologies and services in the future. Moreover, when conducting Metaverse discussions from a multifaceted perspective, a more nuanced approach is particularly necessary in addressing potential risks.

In the context of Metaverse risks, while research conducted from an objective perspective by experts in previous studies has been valuable, it is equally important to understand Metaverse technologies, services, and associated risks based on the subjective experiences and perceptions of actual Metaverse users. This is because even the most advanced and evolved technologies are ultimately centered on the users who utilize them. By approaching risk issues from the perspective of users' perceptions and real-world experiences, it

becomes possible to engage in practical discussions that can lead to solutions for emerging problems. Furthermore, the outcomes of these discussions on Metaverse risks can pave the way for the stable diffusion and development of Metaverse technologies and services in line with the initial expectations and intentions of our society.

Building upon these theoretical discussions and considerations, this study aims to find out the risks and threats inherent in Metaverse technologies and services. It seeks to concretize and categorize the risks arising from the use of Metaverse technologies and services, positioning itself as an extension of digital media risk research and the beginning of Metaverse risk research. Furthermore, this study intends to conduct empirical research centered on the experiences and perceptions of actual service users regarding the risks associated with the use of Metaverse technologies and services. Based on the previous problem awareness, the research question is as follows.

RQ1. What are the risks that emerge in Metaverse environments?

First, RQ1 aims to specify what risks occur when using the Metaverse. Additionally, the purpose is to reclassify the risks that have been specified as a whole, focusing on the characteristics and nature of the risks. This is because the risks that occur when using the Metaverse are perceived as new but not entirely new. Therefore, a comprehensive literature review is conducted, from traditional digital media risks to new types of digital service risks. Next, the reliability and validity of the risk factors are enhanced by conducting in-depth interviews with Metaverse heavy users based on the risk factors and types identified through the literature review.

RQ2. What are the perceived risks of Metaverse users?

RQ2 aims to identify the actual risk perceptions of users regarding the risk factors identified in the first research question. To achieve this, the study will measure the Risks Occurrence Perception and Risks Seriousness Perception among users who have experience using actual Metaverse platforms. The product of these two values will be used to assess the level of user risk perception. Furthermore, the study will discuss the priority of risks that urgently require risk response based on this user risk perception.

3. Research method

To assess the risk perceptions of Metaverse users, this study employed a quantitative methodology, a widely used research approach in the social sciences. Considering the popularity and scalability of Metaverse technologies and services, it was deemed appropriate to evaluate risk perceptions among a large number of users and engage in discussions based on the findings. Consequently, a survey was conducted as the primary research method.

3.1. Sampling

The survey for this study was conducted through panel data from Embrain, an online research company. The survey was conducted over over the course of 6 days, from August 17 to 23, 2023, and targeted 750 respondents. In total, excluding 35 unusable responses were identified. These non-diligent responses were removed, 715 out of the 750 valid responses were included. The survey respondents were recruited from all adults aged 19 or older, and were limited to users who have experience using at least one of the representative Metaverse platforms currently in service in Korea, including <Roblox>, <Zepeto>, and <ifland>.

While a diverse range of Metaverse platforms are currently available, this study focuses on three specific platforms: <Roblox>, <Zepeto>, and <ifland>. This decision was made

after thoroughly reviewing prior research on the Metaverse, which consistently identified these three services as representative platforms (Jeon, 2021; Choi & Lee, 2021).

Furthermore, this study specifically focuses on three Metaverse platforms due to their nature as complex services that converge games and real-life activities (Son et al, 2023). This distinction sets them apart from traditional game-oriented Metaverse platforms, which have primarily focused on individualistic aspects and entertainment. The convergence of games and real-life activities in these platforms transforms them into extended everyday spaces that transcend the boundaries between the physical and virtual worlds. This unique characteristic makes them particularly relevant to this study's objectives, which aim to examine the reception, risks, and associated impacts of such a convergence.

And lastly, it is important to acknowledge that the Metaverse is still in its early stages of development, with platforms constantly evolving and maturing (Shin & Park, 2023). For the aforementioned reasons, this study deliberately limits its research subjects to users who have experience using at least one of the three services: <Roblox>, <Zepeto>, and <ifland>.

3.2. Measurement

This study identified risk factors by analyzing previous research on digital media risks and the Metaverse. Based on the analysis, three main categories of potential risks associated with Metaverse platform use were identified: individual risks (Personal risks and Physical-health risks), societal risks, and economic risks. Within each of the three risk categories, a total of 21 specific risk factors were identified.

Metaverse risks in the personal sphere are divided into two sub-risk types: Personal risks and Physical-health risks. Personal risks factors include: Privacy, Cyberbullying and Harassment, Data sovereignty infringement, Surveillance society. Physical-health risks factors include:

Addiction and obsessive behavior, Physical Health Concerns, Mental Health Concerns. Next, societal risks consist of the 12 most numerous detailed risks, include: Information overload, Malicious code and viruses, Illegal and harmful information, Hacking, Digital divide, Internet trolls, Sudden service malfunctions and interruptions, Conflicts between regulation and freedom of expression, Job displacement, Language destruction, Infodemics, Cyber gambling. Lastly, economic risks consist of two types: Financial scams and fraud issues and Intellectual Property and Copyright.

Based on the identified Metaverse risk types and factors, this study developed a measurement tool to assess users' perceived risks level (Song & Kim, 2013). Specifically, this study investigates the measures of risk occurrence perception and risk seriousness perception that users exhibit within the Metaverse environment. The risk perception level is calculated by multiplying the average of these two measures.

In this study, the Risks Occurrence Perception is defined as “the degree to which users perceive that a risk will occur and the extent to which they believe they will suffer harm if it does.” Risks Seriousness Perception is defined as “the urgency of the potential harm caused by the risk associated with using Metaverse platforms.” The measurement of risk perception was adapted from previous studies (Kim & Kim, 2015; Song, 2014) to align with the specific objectives of this research. Consistent with the previous studies, all of the risk factors were measured through the 7-point scale.

4. Results

4.1. Demographic Characteristics

The demographic characteristics of this study are as follows. First, there were 361 male respondents (50.5%) and 354 female respondents (49.5%). The most frequently used Metaverse platform was <Zepeto> (49.0%) followed by

<Roblox> (35.9%), and <ifland> (15.1%).

The average weekly frequency of Metaverse platform use was less than once by 336 participants (47.0%), followed by 1-2 times (33.7%), 3-4 times (13.3%), 5-6 times (3.5%), and 7 or more times (2.5%). The most common primary location for using the Metaverse platform was at home (70.8%), followed by while commuting (16.9%), at school or work (8.7%), at leisure facilities (2.9%), and other locations (0.7%). The most common device used for accessing the Metaverse platform was a smartphone (74.4%), followed by a personal computer (11.6%), a laptop (8.4%), a tablet PC (5.3%), and a gaming console (0.3%).

Table 3
Demographic of Study Participants

Variables	Description	Frequency	Percentages
Gender	Male	361	50.5
	Female	354	49.5
age	20-29	259	36.2
	30-39	218	30.5
	40-49	186	26.0
	50-	52	7.3
Main use Metaverse platform	Roblox	257	35.9
	Zepeto	350	49.0
	ifland	108	15.1
Main place of use	home	506	70.8
	school or work	62	8.7
	while commuting	121	16.9
	leisure facilities	21	2.9
	Etc	5	0.7
Device	smartphone	532	74.4
	laptop	60	8.4
	PC	83	11.6
	tablet PC	38	5.3
	gaming console	2	0.3
Average Weekly Usage	Less than once	336	47.0
	1-2	241	33.7
	3-4	95	13.3
	5-6	25	3.5
	7-	18	2.5
Total		715	100

4.2. Reliability Analysis

Table 3 presents descriptive statistics for all measures and the dependent variable. It also includes Cronbach's Alpha coefficients for all dimensions of the variables. The alpha values ranged from .78 to .96. In social science research, Cronbach's Alpha is a commonly used measure of internal consistency reliability (Hair et al., 2006).

Table 4
Descriptive Statistics of Measures

Variables	N of Items	M(S.D.)	Cronbach's Alpha
Personal Risks	4	23.14(9.49)	.870
Physical-health Risks	3	22.09(10.85)	.881
Societal Risks	12	22.61(9.09)	.940
Economic Risks	2	23.25(10.98)	.788
Total	21	22.70(8.79)	.961

4.3. Descriptive Statistics of Risk Perception

4.3.1. Descriptive Statistics of the Risks Occurrence Perception

This study examined the Risks Occurrence Perception by risk type among Metaverse platform users. The findings revealed that Economic Risks ($M = 4.77$, $SD = 1.27$) were perceived as having the highest likelihood of occurrence, followed by Personal risks ($M = 4.73$, $SD = 1.10$), Societal Risks ($M = 4.66$, $SD = 1.03$), and Physical-health risks ($M = 4.59$, $SD = 1.34$).

A further analysis of the Risks Occurrence Perception by specific risk type revealed that Cyberbullying and Harassment ($M = 5.11$, $SD = 1.36$) was perceived as having the highest likelihood of occurrence among Metaverse users. This was followed by concerns about Hacking ($M = 4.96$, $SD = 1.38$), Illegal and harmful information ($M = 4.91$, $SD = 1.43$), Conflicts between regulation and freedom of expression ($M = 4.88$, $SD = 1.38$), Internet trolls ($M = 4.88$, $SD = 1.42$), Information overload ($M = 4.86$, $SD = 1.42$), Language destruction ($M = 4.83$, $SD = 1.52$), and Financial scams and fraud issues ($M = 4.79$, $SD = 1.47$).

Table 5

Summary of Descriptive Statistics of the Risks Occurrence Perception

	Variables	M(S.D.)
Individual Risks	Personal risks	4.73(1.10)
	Privacy	4.56(1.32)
	Cyberbullying and Harassment	5.11(1.36)
	Data sovereignty infringement,	4.61(1.34)
	Surveillance society	4.65(1.43)
	Physical-health risks	4.59(1.34)
	Addiction and obsessive behavior	4.73(1.51)
	Physical Health Concerns	4.63(1.52)
	Mental Health Concerns	4.41(1.55)
	Average	4.66(1.03)
Societal Risks	Information overload	4.86(1.42)
	Malicious code and viruses	4.76(1.48)
	Illegal and harmful information	4.91(1.43)
	Hacking	4.96(1.38)
	Digital divide	4.26(1.53)
	Internet trolls	4.88(1.42)
	Sudden service malfunctions and interruptions	4.43(1.38)
	Conflicts between regulation and freedom of expression	4.88(1.38)
	Job displacement	4.09(1.44)
	Language destruction, Infodemics	4.83(1.52)
Economic Risks	Cyber gambling	4.68(1.47)
	Cyber gambling	4.45(1.59)
	Financial scams and fraud issues	4.79(1.47)
	Intellectual Property and Copyright	4.76(1.40)
	Average	4.77(1.27)

4.3.2. Descriptive Statistics of the Risks Seriousness Perception

This study also measured Metaverse platform users' Risks Seriousness Perception. The findings revealed that Personal risks ($M = 4.62$, $SD = 1.21$) were perceived as having the most severe consequences, followed by Economic Risks ($M = 4.57$, $SD = 1.35$), Societal Risks ($M = 4.54$, $SD = 1.13$), and Physical-health risks ($M = 4.47$, $SD = 1.35$).

A further analysis of users' Risks Seriousness Perception by specific risk factors revealed that Cyberbullying and Harassment ($M = 4.87$, $SD = 1.45$) was perceived as having the most severe consequences. This was followed by concerns about Language destruction ($M = 4.82$, $SD = 1.51$), Internet trolls ($M = 4.79$, $SD = 1.41$),

Illegal and harmful information ($M = 4.76$, $SD = 1.45$), information overload ($M = 4.71$, $SD = 1.43$), Conflicts between regulation and freedom of expression ($M = 4.71$, $SD = 1.40$), Hacking ($M = 4.69$, $SD = 1.44$), Financial scams and fraud issues ($M = 4.61$, $SD = 1.49$), and Infodemics ($M = 4.59$, $SD = 1.48$). These findings indicate that Metaverse users are particularly concerned about the potential negative impacts of these specific risks on their safety, privacy, well-being, and ability to communicate and express themselves freely.

Table 6

Summary of Descriptive Statistics of the Risks Seriousness Perception

	Variables	M(S.D.)
Individual Risks	Personal risks	4.62(1.21)
	Privacy	4.58(1.36)
	Cyberbullying and Harassment	4.87(1.45)
	Data sovereignty infringement,	4.54(1.38)
	Surveillance society	4.51(1.46)
	Physical-health risks	4.47(1.35)
	Addiction and obsessive behavior	4.55(1.51)
	Physical Health Concerns	4.45(1.53)
	Mental Health Concerns	4.41(1.52)
	Average	4.54(1.13)
Societal Risks	Information overload	4.71(1.43)
	Malicious code and viruses	4.56(1.47)
	Illegal and harmful information	4.76(1.45)
	Hacking	4.69(1.44)
	Digital divide	4.16(1.54)
	Internet trolls	4.79(1.41)
	Sudden service malfunctions and interruptions	4.30(1.41)
	Conflicts between regulation and freedom of expression	4.71(1.40)
	Job displacement	4.01(1.50)
	Language destruction, Infodemics	4.82(1.51)
Economic Risks	Cyber gambling	4.59(1.48)
	Cyber gambling	4.33(1.55)
	Financial scams and fraud issues	4.61(1.49)
	Intellectual Property and Copyright	4.54(1.46)
	Average	4.57(1.35)

4.3.3. Descriptive Statistics on Perceived Risks

Risk assessment scores were computed by multiplying the mean values of the Risks Occurrence Perception and Risks Seriousness

Perception factor. The analysis revealed that Cyberbullying and Harassment exhibited the highest overall risk assessment score ($M = 26.17$, $SD = 11.94$). This suggests that Metaverse users perceive avatar-directed violence as the most probable and consequential threat compared to other identified risk factors.

Following Cyberbullying and Harassment, Language destruction ($M = 24.75$, $SD = 12.55$) emerged as another significant risk factor, highlighting concerns about the potential for linguistic manipulation and erosion of cultural norms within the Metaverse. The Illegal and harmful information ($M = 24.69$, $SD = 12.04$) also garnered high risk assessment scores, underscoring the challenges of content moderation and safeguarding users from exposure to harmful material. Similarly, Internet trolls ($M = 24.65$, $SD = 11.82$) and Hacking ($M = 24.52$, $SD = 11.62$) were identified as prevalent concerns among Metaverse users.

The study further revealed that the Conflicts between regulation and freedom of expression ($M = 24.20$, $SD = 11.51$) posed a significant risk, reflecting the complexities of balancing user autonomy with the need for effective governance within the Metaverse. Information overload ($M = 24.14$, $SD = 11.50$) emerged as another prominent concern, highlighting the potential for cognitive strain and decision fatigue associated with the vast amount of data and stimuli encountered in the Metaverse.

Financial scams and fraud issues ($M = 23.54$, $SD = 12.25$) were also perceived as a major risk, emphasizing the vulnerability of users to financial fraud and scams within the virtual realm. The distribution of Malicious code and viruses ($M = 23.08$, $SD = 11.90$) and Intellectual Property and Copyright ($M = 22.96$, $SD = 11.92$) further underscored the cyber security threats prevalent in the Metaverse.

Concerns about Addiction and obsessive behavior ($M = 22.96$, $SD = 12.14$), Infodemics ($M = 22.90$, $SD = 11.96$), and the potential for a Surveillance society ($M = 22.27$, $SD = 11.45$) also

emerged as significant risk factors. The potential for Physical Health Concerns ($M = 22.22$, $SD = 12.13$), Data sovereignty infringement ($M = 22.10$, $SD = 10.82$), Privacy ($M = 22.03$, $SD = 10.48$), Mental Health Concerns ($M = 21.08$, $SD = 11.95$), Cyber gambling ($M = 20.98$, $SD = 12.38$), Sudden service malfunctions and interruptions ($M = 20.27$, $SD = 10.69$), and the Digital divide ($M = 19.32$, $SD = 11.58$) were also identified as potential risks.

Interestingly, the risk assessment score for Job displacement ($M = 17.86$, $SD = 10.88$) was the lowest among the evaluated factors. This suggests that Metaverse users may be relatively less concerned about the occupational implications of technological advancements within the virtual environment.

Table 7
Summary of Descriptive Statistics of Perceived Risks

	Variables	M(S.D.)
Individual Risks	Personal risks	23.14(9.49)
	Privacy	22.03(10.48)
	Cyberbullying and Harassment	26.17(11.94)
	Data sovereignty infringement,	22.10(10.82)
	Surveillance society	22.27(11.45)
	Physical-health risks	22.09(10.85)
	Addiction and obsessive behavior	22.96(12.14)
	Physical Health Concerns	22.22(12.13)
	Mental Health Concerns	21.08(11.95)
	Information overload	24.14(11.50)
	Malicious code and viruses	23.08(11.90)
	Illegal and harmful information	24.69(12.04)
	Hacking	24.52(11.62)
	Digital divide	19.32(11.58)
	Internet trolls	24.65(11.82)
Societal Risks	Sudden service malfunctions and interruptions	20.27(10.69)
	Conflicts between regulation and freedom of expression	24.20(11.51)
	Job displacement	17.86(10.88)
	Language destruction,	24.75(12.55)
	Infodemics	22.90(11.96)
	Cyber gambling	20.98(12.38)
	Average	22.61(9.09)
Economic Risks	Financial scams and fraud issues	23.54(12.25)
	Intellectual Property and Copyright	22.96(11.92)
	Average	23.25(10.98)

5. Discussions

This research aims to understand the Metaverse technology and services that are gaining high attention in the media industry and market for their high potential for development. It endeavors to not only cultivate a comprehensive understanding of the Metaverse ecosystem but also to illuminate the inherent risks associated with Metaverse platforms. This risk identification serves the critical purpose of fostering the sustainable development and proliferation of the Metaverse industry. Recognizing the Metaverse's unique characteristic – its user-centricity surpassing that of any other digital media service – this study adopts a user-centered approach to explore risk perception.

The impetus for this study stems from the burgeoning ubiquity of Metaverse technology within our everyday lives and professional spheres. This pervasiveness is fueled by the technology's ever-expanding range of applications and escalating market potential. However, this rapid integration necessitates a critical exploration of the inherent risks associated with this double-edged sword. The unfettered adoption of Metaverse technology has the potential to transform our society into a 'risk society,' characterized by pervasive anxieties and uncertainties.

Furthermore, despite the fervent expectations surrounding Metaverse technology and services, a crucial consideration remains. As evidenced by prior research conducted by Riek, Bohme, & Moore (2015) and Al-Adwan et al. (2023), the nascent risks associated with this technology could potentially impede both technological advancement and industrial progress. This study is designed to investigate and illuminate these potential risks.

Based on the identified concerns, this study conducted a comprehensive risk assessment of the Metaverse. The findings revealed a spectrum of potential risks associated with this emerging technology. However, considering the rapid pace of Metaverse industry development and

the competitive landscape, it is imperative to prioritize and address the factors with the highest risk ratings rather than formulating overarching strategies for all identified risks.

A key finding is the necessity to prioritize risk management strategies. This prioritization should focus on those risk factors with high assessed risk, particularly those related to user-perceived economic risks. This emphasis is even more critical considering the predicted emergence of robust virtual economies within future Metaverse platforms.

Firstly, for issues like copyright infringement of intellectual property, continuous monitoring and enforcement are crucial. This includes identifying and stopping such violations through robust monitoring mechanisms, alongside user education and public awareness campaigns. These campaigns can highlight the importance of respecting intellectual property rights in the Metaverse, fostering a culture of responsible behavior.

Secondly, for areas where legal recourse exists, such as copyright infringement or cyber financial crimes, a stricter approach is necessary. This entails a "no-tolerance policy" towards violations. This means swift action against offenders, including content removal and potential legal consequences. Collaboration with law enforcement is also vital to investigate and prosecute serious cases, demonstrating a strong governmental commitment to eradicating such activities.

Next is the response to specific risk factors, particularly Cyberbullying and Harassment. The study identifies Cyberbullying and Harassment as a critical risk factor demanding urgent attention in the Metaverse. This is due to the high likelihood of occurrence and the severity of potential consequences for users. Furthermore, as Metaverse technology advances, offering heightened immersion and realism, cyberbullying is likely to inflict even greater psychological and potentially physical harm.

Considering these points, a specific

measure for cyberbullying and harassment is to improve the stability of the Metaverse environment based on investment in the technological aspect. In other words, in order to manage and supervise crimes targeting avatars occurring in the Metaverse environment and further create a preventive effect, we must invest in AI technology to develop and introduce an intelligent risk detection system, thereby securing stability in the Metaverse environment. By implementing a multi-pronged approach that combines technological advancements and accessible support systems, we can create a safer and more respectful Metaverse environment. This will not only protect individual well-being but also foster a more positive and productive virtual society.

To sum up, in light of users' high risk assessments associated with Metaverse usage, a multifaceted approach is necessary. This entails both micro-level responses to specific risks and macro-level strategies aligned with the overall risk landscape. By implementing a multi-pronged approach that combines prioritized micro-level responses, comprehensive macro-level strategies, and ongoing research and development, we can transform the Metaverse from a perceived "risk society" into a safe and secure virtual society. This will not only protect individual well-being but also foster a thriving and productive Metaverse environment for all users.

The findings and recommendations of this study have significant implications for future research and practice in the realm of Metaverse risks. Prior research on digital risks, despite its growing importance, has largely focused on individual risks in isolation, failing to capture the interconnectedness and holistic nature of these threats. This study addresses this limitation by expanding the scope of early digital risk research discussions to encompass the Metaverse.

For this reasons, this study comprehensively identifies and characterizes various risk factors associated with Metaverse platform usage. It goes beyond simply listing

individual risks and attempts to understand the overall risk landscape by categorizing risks based on shared characteristics. This holistic approach provides a more comprehensive understanding of the diverse risk factors arising from Metaverse technologies and services.

The study's findings serve as a valuable theoretical framework for future discussions on Metaverse technology and service risks. It offers a structured approach for examining and analyzing emerging threats in the Metaverse. Moreover, the study's methodology can be employed to investigate risks associated with other new media technologies and services, fostering a more evolved and integrated approach to risk assessment and mitigation.

In summary, this study contributes to the understanding of Metaverse risks by providing a comprehensive overview of potential threats, categorizing risks based on shared characteristics, and offering a theoretical framework for future research. Its findings can inform the development of effective risk mitigation strategies and promote a safer and more secure Metaverse environment for all users.

This study further distinguishes itself through its user-centric empirical approach. Instead of solely relying on a theoretical listing of potential Metaverse risks, this research actively investigates user experiences and perceptions. This approach is particularly relevant given the user-driven nature of Metaverse technologies and services. User research is paramount to understanding Metaverse industry and its associated risks.

Furthermore, as the Metaverse gains traction, social debates surrounding potential risks have intensified. This study addresses this critical need by diagnosing these risks based on user perceptions and lived experiences. This user-centered approach to risk identification and impact assessment holds significant academic value, as it provides valuable insights for developing effective risk mitigation strategies and fostering a safer Metaverse experience.

6. Limitations

To enhance the generalizability of the study's findings, a quantitative survey method was employed. However, the use of panel data from a specific survey institution for participant recruitment limits the representativeness of the sample. Future research on Metaverse users should diversify participant collection and selection methods to improve the generalizability of results.

Due to recruitment convenience, the study focused on adult users aged 20 and above, excluding teenage users. However, considering that teenagers are the primary users of Metaverse platforms, their inclusion in future research is crucial. This limitation could affect the generalizability and trustworthiness of the findings. Therefore, subsequent studies should include teenagers, the main user group of Metaverse platforms, to investigate their risk perceptions and experiences.

References

- Ahn, Jae-Hyeon., Kwon, Jae Won., Kim, Myung Soo., Lee, Dong Joo., Lee, Sang Youn., & Han, Sang Pil. (2002). An Exploratory Study for the Telecommunications Service Failure Cases in South Kores. *Journal of the Korean Operations Research and Management Science Society*, 27(3), 115-134.
- Al-Adwan, A. S., Li, N., Al-Adwan, A., Abbasi, G. A., Albelbisi, N. A., & Habibi, A. (2023). Extending the technology acceptance model (TAM) to Predict University Students' intentions to use metaverse-based learning platforms. *Education and Information Technologies*, 1-33.
- Bale, A. S., Ghorpade, N., Hashim, M. F., Vaishnav, J., & Almaspoor, Z. (2022). A comprehensive study on metaverse and its impacts on humans. *Advances in Human - Computer Interaction*, 2022(1), 3247060.
- Ball, M. (2022). The metaverse: and how it will revolutionize everything. Liveright Publishing.
- Ban, Hyungkul. & Nam, Yoonjae. (2023). A Study on Cyber Violence and Legal Protection in Metaverse: Focusing on Violence Against Avatars. *Korean Journal of Communication Studies*, 31(1), 119-146, <https://doi.org/10.23875/kca.31.1.5>
- Barrera, K. G., & Shah, D. (2023). Marketing in the Metaverse: Conceptual understanding, framework, and research agenda. *Journal of Business Research*, 155, 113420.
- Beck, U. (1992). *Risk Society: Towards a New Modernity*. SAGE Publications.
- Berger, A., Schlager, T., Sprott, D. E., & Herrmann, A. (2018). Gamified interactions: whether, when, and how games facilitate self-brand connections. *Journal of the Academy of Marketing Science*, 46, 652-673.
- Bhardwaj, A. (2024). Navigating the Metaverse: Forecasting Cybercrime in the New Age of Virtual Reality. In *Forecasting Cyber Crimes in the Age of the Metaverse* (pp. 33-65). IGI Global.
- Bobier, J., Merey, T., Robnett, S., Grebe, M., Feng, J., Rehberg, B., Woolsey, K. & Hazan, J. (2022). The Corporate Hitchhiker's guide to the metaverse. Boston Consulting Group, 1-15.
- Bogicevic, V., Liu, S. Q., Seo, S., Kandampully, J., & Rudd, N. A. (2021). Virtual reality is so cool! How technology innovativeness shapes consumer responses to service preview modes. *International Journal of Hospitality Management*, 93, 102806. in press.
- Book, B. (2004). These bodies are FREE, so get one NOW!: Advertising and branding in social virtual worlds. Available at: <https://doi.org/10.2139/ssrn.536422>.
- Cho, Yusun, & Moon, Ahram (2023). The Effects of Prior Knowledge and Experience on Intention to Use Metaverse: Focusing on Path Analysis of Positive, Negative, and Risk Awareness with Service Use Intention. *Journal of Cybercommunication Academic*

- Society, 40(1), 229-276, 10.36494/JCAS.2023.03.40.1.229
- Cho, H. M. (2011). Introduction of Digital Media and Consequent New Risk Types -Focus on the Analysis of User Risk Perception and Risk Features of Smart Phones as Convergence Media-. The Journal of the Korea Contents Association. The Korea Contents Association. <https://doi.org/10.5392/jkca.2011.11.8.353>
- Cho, Hang-Min., & Kim, Chan-Won. (2016). Top 10 Risks of Science and Technology. Communication books.
- Choi, Eunjin. & Lee, Young-suk. (2021). A Study on the Planning of Minhwa Museum Utilizing the Metaverse Platform: Focusing on Zepeto Case. Journal of Korea Game Society, 21(6), 63-74, 10.7583/JKGS.2021.21.6.63
- Choung, Wan. (2007). Current Situation and Criminal Subject of Cybercrime. KOREAN CRIMINOLOGICAL REVIEW, 1499-1535.
- Choung, Wan. (2022). A Study on Legal Issues in Metaverse. Kyung Hee Law Journal, 57(1), 143-170. 10.15539/KHLJ.57.1.5
- Dwivedi, Y. K., Hughes, L., Baabdullah, A. M. et al. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 66, 1-55, <https://doi.org/10.1016/j.ijinfomgt.2022.102542>.
- Dwivedi, Y. K., Kshetri, N., et al. (2023). Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. 25, 2071-2114, <https://doi.org/10.1007/s10796-023-10400-x>.
- Flavián, C., Ibáñez-Sánchez, S., & Orús, C. (2019). The impact of virtual, augmented and mixed reality technologies on the customer experience. Journal of business research, 100, 547-560.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). Multivariate data analysis (Vol. 6). Upper Saddle River, NJ: Pearson Prentice hall.
- Health & Safety Executive. (1998). Five steps to risk assessment. HSE.
- Hong, S. T. (2005). A study on the advent of the information risk society and responses. Korea Information Society Development Institute, Policy and Research Data, 1-109.
- Hur, Jinsung. (2010). A Study on the Problem of SNS's Infringement of Personal Information and its Countermeasures. Journal of Media Law, Ethics and Policy Research, 9(2), 75-103.
- Hwang, Tae Jeong. (2023). Metaverse and Personality Rights in Cyberspace - Review of Current Laws and Bills. Comparative Criminal Justice Studies, 24(4), 157-186.
- Jang, Jin Sook. (2015). Discussion on the Conflict with Intelligence Human Rights: Emphasis on Rights to be forgotten. Korean Journal of Law & Society, 48(0), 167-216.
- Jeon, JoonHyun. (2021). A study on the Principle of Metaverse Composition with a focus on Roblox. korean association for visual culture,(38), 257-279.
- Kang, Jinsuk. (2002). A Study on Digital divide and Respondent Policies of the Internet Network: Focusing on Cases in America and Germany. Korean Journal of Journalism & Communication Studies, 46(4), 5-45.
- Katterbauer, K., Syed, H., & Cleenewerck, L. (2022). Financial cybercrime in the Islamic finance metaverse. Journal of Metaverse, 2(2), 56-61.
- Kim, ChanWon., & Kim, SeokIlKim. (2007). The effect of health risks and severity factors on decisional balance and perceived risk in internet health information users. The Korean Journal of Physical Education, 46(3), 115-125.
- Kim, Dae Gun. (2022). A Study on Ethics for Preventing Sexual Violence in Metaverse. Journal of Ethics Education Studies,(66), 63-90,

<https://doi.org/10.18850/JEES.2022.66.03>

- Kim, Hyung-Jun., & Oh, Se-Gu. (2019). Effects of Gender Difference and Perceived Risk on Acceptance Intention of Mobile Easy Payment Service. *Journal of Management and Economics*, 41(3), 145-165.
- Kim, W. J., & Kim, C. W. (2015). Effect of Trust Toward Digital Risk Management Organization on Risk Perception and Cognition of Risk Management: Focused on Expert Survey. *Journal of Korean Society for Internet Information*, 16(4), 83-91. <https://doi.org/10.7472/jksii.2015.16.4.83>
- Kwon, Jun-I., & Cha, Yong Jin. (2021). Risk Perception in Intelligent Information Society and Policy Implications: A Comparison with Experts and the General Public. *The Journal of Korean Policy Studies*, 21(2), 51-69, 10.46330/jkps.2021.6.21.2.51
- Lee, Chang-Min. (1999). Study on virtual reality and its side effects. *Korea Multimedia Society*, 3(1), 108~117.
- Lee, Chulnam. (2021). A study on copyright issues in Metaverse - Focusing on the spatial data of digital twin. *Journal of Business Administration & Law*, 31(4), 463-493.
- Lee, Dongwoo., & Jinyoung Min. (2021). A Study on the Fraud Detection in an Online Second-hand Market by Using Topic Modeling and Machine Learning . *Information Systems Review*, 23(4), 45-67.
- Lee, Ju Yoen. (2022). A Study on the Solutions to International Copyright Disputes arising from the Metaverse Environment. *Korea Private International Law Journal*, 28(2), 259-299, 10.38131/kpilj.2022.12.28.2.259
- Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Kumar, A. Bermejo, C., & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint arXiv:2110.05352*
- Lee, Sangho., & Cho, Yun Young (2015). A Study on the Measures to Reinforce South Korea's National Defense in Cyber Space in the Age of IoT (Internet of Things). *The Journal of Political Science & Communication*, 18(2), 1-30, 10.15617/psc.2015.06.18.2.1
- Lee, Won Sang. (2022). A Study on the Role of criminal law in Metaverse. *Cnulawreview*, 42(3), 177-202. 10.38133/cnulawreview.2022.42.3.177
- Lee, Won-Tae., Kim, Jeong-Eon., Lee, Si-Jik., Kim, Do-Seung., Cheong, & Kyung-Oh. (2016). A Study on Legal Issues of ICT and Its Policy Implications in the Era of the Fourth Industrial Revolution. *Korea Legislation Research Institute, Global Legislation Research*, 16-20-10, 1-338.
- Molenda, Z. A., Marchlewska, M., Rogoza, M., Michalski, P., Górski, P., Szczepańska, D., & Cislak, A. (2022). What makes an Internet troll? On the relationships between temperament (BIS/BAS), Dark Triad, and Internet trolling. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 16(5).
- National Information Society Agency(2020.12.). *Cyber Violence Survey*. 1-234.
- Park, Ahran. (2022), Discussion on Violation of Personal Rights and Responses in the Metaverse, *Press Arbitration Commission*, 32-39.
- Park, Jang-Hyuk., Jung, Jae-Hun., Kim, Sin-Ryeong., & Kim, Young-Gon. (2016). Research on Automatic Translation of Standard Language through Contemplation of Korean Destruction Phenomena in Internet Media Language. *The Journal of The Institute of Internet, Broadcasting and Communication*, 16(1), 273-281.
- Ryu, Bugon. (2022). Criminal Policy Discussion on Metaverse - Establishment of Cyber Personal Rights Concept and Types of Infringement -. *Korean Journal Of Criminology*, 34(2), 7-42.
- Shafik, W. (2024). Predicting Future Cybercrime Trends in the Metaverse Era. In *Forecasting Cyber Crimes in the Age of the Metaverse*

- (pp. 78-113). IGI Global.
- Shin, Sunkyung., & Park, Joo-Yeun. (2023). A study on Continuous Use Intention of Metaverse Platform through Expectancy Value Theory. *Information Society & Media*, 24(2), 41-78, 10.52558/ISM.2023.08.24.2.41
- Slovic, P. (1992). Perception of risk: Reflections on the psychometric paradigm.
- So, Wongeun., & Kim, Hakyun. (2017). Effects of Information Overload to Information Privacy Protective Response in Internet of Things(Iot). *Management and Information Research*, 36(1), 81-94.
- Son, Beom-Sik., Son, Sung-Bin., & Kim, Geon-Dong. (2023). Meta Surf: A Metaverse Travel Platform That Connects Real and Virtual Space-Time Coordinates. *Journal of Digital Contents Society*, 24(6), 1229-1241, 10.9728/dcs.2023.24.6.1229
- Song, G. (2014). Understanding public perceptions of benefits and risks of childhood vaccinations in the United States. *Risk Analysis*, 34(3), 541-555.
- Song, Hae-Ryong., & Kim, Won-Je. (2013). Effects of Risk Characteristic and Risk Perception on Risk Severity of Natural Disaster. *JOURNAL OF THE KOREA CONTENTS ASSOCIATION*, 13(4), 198-207.
- Stephenson, N. (1992). *Snow Crash*. New York: Bantam Books.
- Vig, S. (2022). Intellectual property rights and the metaverse: An Indian perspective. *The Journal of World Intellectual Property*, 25(3), 753-766.
- Wang, H., Ning, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2023). A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. *IEEE Internet of Things Journal*, 10(16), 14671-14688.
- Wei, W., Qi, R., & Zhang, L. (2019). Effects of virtual reality on theme park visitors' experience and behaviors: A presence perspective. *Tourism management*, 71, 282-293.
- Yun, Sang-Oh. (2013). A Study on the Classification of Risks Caused by Big Data. *Journal of Korean Association for Regional Information Society*, 16(2), 93-122.
- Yun, Yeo-Saeng., & Yu, Jin-Ho. (2012). Analysis of Trends in Laws and Regulations on Illegal and Harmful Information. *Korea Institute of Information Security and Cryptology*, 22(3), 25-36.