

## Article

# Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety

Mohamed Chawki <sup>1</sup>, Subhajit Basu <sup>2</sup> and Kyung-Shick Choi <sup>3,\*</sup>

<sup>1</sup> Criminal Law Department, Naif Arab University for Security Sciences, Riyadh 11452, Saudi Arabia; mshaker@nauss.edu.sa

<sup>2</sup> School of Law, University of Leeds, Leeds LS2 9JT, UK; s.basu@leeds.ac.uk

<sup>3</sup> Metropolitan College, Boston University, Boston, MA 02215, USA

\* Correspondence: kuung@bu.edu

**Abstract:** This paper analyses sexual crimes within the Metaverse to develop an effective legal framework. The aim is to enhance safety in virtual realities, ensuring the Metaverse remains a secure, respectful, and liberating environment for all users. As the Metaverse continues to evolve, merging augmented physical reality with digital existence, it introduces new opportunities for socialisation, commerce, education, and entertainment. However, this digital realm also faces significant challenges, particularly the increase in sexual violence. This article evaluates the development of the Metaverse and its impact on sexual offences. It provides an overview of the Metaverse, followed by an in-depth exploration of the nature of sexual violence in this virtual space, its effects on victims, and the resulting legal and ethical issues. Additionally, this article examines the complexities of combating sexual violence within the Metaverse, reviewing the legal frameworks in various jurisdictions, including the United States, the European Union, the United Kingdom, and South Korea. These examinations reveal a range of legal viewpoints and possible solutions. This article outlines a proposed legal framework, highlighting key strategic areas for mitigating sexual violence in the Metaverse. The primary objective is to enrich the discourse on the Metaverse, pushing for strong, flexible, and holistic legal measures. Through this research, we aim to contribute to the creation of protective mechanisms against sexual violence in these emerging virtual landscapes.

**Keywords:** Metaverse; sexual violence; legal challenges; international law; regulation; legal framework; USA; EU; South Korea



**Citation:** Chawki, Mohamed, Subhajit Basu, and Kyung-Shick Choi. 2024. Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws* 13: 33. <https://doi.org/10.3390/laws13030033>

Academic Editors: Esther Salmerón-Manzano and Francisco Manzano Agugliaro

Received: 24 February 2024

Revised: 20 May 2024

Accepted: 21 May 2024

Published: 24 May 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The advent of the Metaverse signifies a paradigmatic shift in the human–computer interaction. This convergence of augmented physical reality with a persistent virtual existence offers unparalleled opportunities for socialisation, commerce, education, and entertainment. However, this expansive digital domain is not devoid of significant challenges. Among these, the emergence of sexual violence within the Metaverse stands out as a pressing and urgent issue that demands immediate attention. This troubling phenomenon exploits the very technological innovations that define the unique characteristics of the Metaverse.

This paper provides an in-depth analysis of the development of the Metaverse, with a specific focus on the misuse of emerging technologies for sexual offences. It begins with a critical evaluation of the extensive body of literature surrounding the complex dimensions of Metaverse development. This evaluation covers technological foundations, ethical dilemmas, security and privacy challenges, and legal and governance frameworks to ensure a safe environment and prevent criminal activities. The Methodology Section details our approach to these issues through a doctrinal legal perspective. Utilising comparative legal analysis, we investigate the issue of sexual violence in the Metaverse across four distinct legal jurisdictions including the United States, the European Union, the United Kingdom, and South Korea. This methodology enables us to uncover and understand the

subtleties of legal challenges across these jurisdictions and to formulate comprehensive solutions to these intricate issues. Our structured analysis aims to offer insights into effective legal mechanisms that could reduce the incidence of sexual violence within the Metaverse, identifying both existing gaps and possible improvements. We propose a preliminary legal framework aimed at reducing sexual violence in the Metaverse. This framework is intended to highlight strategic areas essential for addressing this issue in the digital realm. The primary goal of this paper is to contribute significantly to the ongoing discourse about the Metaverse, specifically in the context of sexual violence, and to underscore the need for robust, flexible, and comprehensive legal frameworks. Through our investigation, we seek to outline the challenges and aid in developing solutions that ensure the Metaverse is a safe, dignified, and accessible environment for all its users.

## 2. Literature Review

The concept of the Metaverse has garnered significant attention in recent years, with scholars exploring various aspects of this emerging digital realm from interdisciplinary perspectives. A common theme across the reviewed literature is the need for a comprehensive strategy to address the challenges the Metaverse poses, particularly regarding security, privacy, governance, and ethical considerations. This strategy encompasses adopting innovative platforms for safety training alongside integrating virtual reality technology to augment conventional safety training techniques (Fajar et al. 2022).

Despite these advancements, the inherent risk of criminal activities within these virtual environments necessitates a holistic approach to safety. This includes implementing stringent security measures, establishing reliable identity verification systems, and developing robust infrastructure to support Metaverse operations (Gu et al. 2023). The formulation of evidence-based policies and interventions plays a crucial role in minimising the adverse effects of the Metaverse on individual well-being and ensuring a secure virtual space for all participants.

Qin et al. (2022) argued for creating an international legal framework to enhance global collaboration, facilitate crime investigations, and foster democratic governance within the Metaverse. They emphasised the critical role of identity in this virtual realm and proposed a decentralised governance model, leveraging blockchain technology and transparent AI algorithms to ensure democracy. This strategy recognises the Metaverse's disregard for geographical boundaries and seeks to address the challenges it presents to traditional legal frameworks. Lee et al. (2021) highlighted the vital role of legislative bodies in soliciting and analysing feedback from various stakeholders, including industries, users, and expert groups, to prevent the negative consequences of hastily enacted legislation. They identified breaches of personal information and digital sex crimes as significant security concerns within the Metaverse, recommending that the legal system be revised within the context of existing laws rather than creating new, separate legislation. This thoughtful approach balances the need for security against the potential negative impact of overly harsh sanctions on the Metaverse industry.

Marshall and Tompsett (2023) challenge the notion of the Metaverse as a revolutionary advancement, suggesting that while it may not create new forms of abusive behaviour or crime, it can amplify existing issues on a larger scale. This nuanced perspective requires a balanced understanding of the ethical implications of immersive online experiences. Fajar et al. (2022) demonstrate the effectiveness of safety training using the Metaverse concept and virtual reality technology, particularly within the shipping industry. Their study, which involves 60 respondents, shows that gender and age do not significantly affect the functionality or usability of virtual reality in safety training, underscoring the Metaverse's potential to enhance work collaboration across geographical areas without demographic limitations. Wu et al. (2023) discuss the challenges posed by the decentralisation of Web3 for governance and the rise of financial crimes in the Metaverse ecosystem. They underscore the importance of comprehensive governance mechanisms to tackle these emerging challenges and protect users from potential threats (ibid.). The lack of industry standards and regu-

latory rules has made Metaverse attractive to financial criminals, highlighting the need for comprehensive governance mechanisms to address these challenges. Laue (2011) explores the conceptual and methodical challenges of analysing deviant behaviour in virtual worlds from a criminological perspective. He suggests that while Metaverse may lead to a quantitative increase in online criminality, they have a low potential for developing entirely new forms of criminality (ibid.). The impact of virtual worlds on user behaviour in real society requires further research. Lee et al. (2021) discuss the auxiliary role of criminal law in addressing crimes within the Metaverse (W. S. Lee 2022). They advocate the integration of crimes from special laws into the criminal code and call for discussions to establish a “Metaverse criminal law system” tailored to the new era. This proposal aims to provide a legal framework to address cybercrimes within the Metaverse effectively. Zhao et al. (2023) analyse the Metaverse as a super 3D VR ecosystem, identifying serious security and privacy concerns that must be addressed (ibid.). They propose potential solutions to these issues, recognising the Metaverse’s benefits in reducing discrimination, eliminating individual differences, and enhancing socialisation.

Kasiyanto and Kilinc (2022) examine the economic potential of the Metaverse, highlighting significant legal considerations around traditional property law, intellectual property law, privacy, and governance structures within this emerging digital realm (ibid.). Similarly, Benrimoh et al. (2022) focus on the transformative potential of the Metaverse in reshaping societal norms through enhanced self-expression and interaction channels (ibid.). They also discuss the Metaverse’s capacity to revolutionise societal norms through unlimited channels of self-expression and interaction. Kalyvaki (2023) addresses the complex legal landscape of the Metaverse, focusing on the intricacies of intellectual property, privacy, and jurisdiction (ibid.). The study underscores the urgent need for a clear definition of virtual asset ownership and advocates interdisciplinary approaches to navigate these legal challenges. Lee et al. (2021) argue for a cautious legislative approach to the Metaverse, emphasising the need for consultation with industry stakeholders, users, and experts to mitigate the adverse effects of precipitous laws (J. H. Lee 2022). They underscore the relevance of existing legal frameworks, such as the Framework Act on Intellectual Property and Related Laws (South Korea), to future legal challenges in the Metaverse. Their study calls for advanced legal preparations to ensure safety and address potential legal problems in the digital space. Allam et al. (2022) examine the Metaverse in the context of smart cities, emphasising the need to prioritise human values and inclusivity in future digital societies. They highlight the disruptive effects of the Metaverse on urban society and stress the importance of reshaping the concept to prioritise human values and ensure inclusivity and accessibility in future digital societies. These analyses suggest a way forward, where a holistic approach to developing and implementing strict measures against any sexual crimes in the Metaverse is required. Preferably, this should involve revising existing legislation rather than introducing new laws to simplify the process while preserving the Metaverse’s potential benefits. The discussions emphasise the necessity of interdisciplinary collaboration, proactive legal preparation, and thoughtful regulation to navigate the complexities of this emerging digital frontier effectively.

### 3. Methodology

This article adopted a doctrinal legal methodology employing comparative legal analysis to investigate challenges thoroughly and formulate comprehensive solutions for sexual violence in the Metaverse (Bhat 2020a, 2020b; Reitz 1998; Vranken 2011). The following subsections elaborate on the approach adopted in this study.

#### 3.1. Data Collection

A comprehensive literature review was carried out across major databases in legal, technology, and social science fields, including Google Scholar, ScienceDirect, ACM Digital Library, IEEE Xplore, PsycINFO, and SocINDEX. The review analysed peer-reviewed articles, conference papers, and book chapters, utilising iterative keyword searches re-

lated to “Metaverse”, “virtual reality”, “sexual assault”, “online harassment”, “content moderation”, and “technology policy”. From the insights gained through the literature review, legal doctrines related to cybersexual violence from the U.S., U.K., EU, and South Korea were methodically identified and collated into a master database. This compilation encompassed statutes, case law, regulations, and directives. The review of legal doctrines across these jurisdictions aimed to evaluate the current approaches to addressing sexual violence in the Metaverse or digital spaces (Keenan and Zinsstag 2022; Wodajo 2022).

Data collection entailed examining statutes, case law, international conventions, and academic literature. We used expertise from criminal law specialists, who analysed different jurisdictional responses to these incidents within the framework of their legal systems, specifically highlighting the challenges posed by the virtual context of the Metaverse.

### 3.2. Analysis

Adopting a comparative law approach (Bhat 2020a; Reitz 1998), this article identified and evaluated the legal responses to virtual sexual violence, focusing on their effectiveness and relevance to the Metaverse. Directed qualitative content analysis methods were employed to critically examine doctrinal data, enabling a comparison of legal approaches across jurisdictions. This analysis aimed to identify gaps in protection, assess the applicability of existing laws to the Metaverse, and outline ethical and safety considerations. Legal scholars have underscored the importance of recognising the shortcomings in current legal protections and the challenges posed by differences in jurisdictional laws. Additionally, the technological aspects crucial for both the perpetration and prevention of such acts were examined in relation to user interactions within Metaverse platforms. For instance, to combat avatar-related sex crimes, some scholars have proposed specific punitive measures and preventive strategies, such as restricting avatars from approaching each other beyond a certain distance (Ye and Chang 2022).

### 3.3. Framework Development

Analysing previous studies and expert opinions enables legislative bodies to gather and analyse feedback from relevant industries, users, and expert groups. This approach ensures the Metaverse is used in a healthy and safe manner, minimising the risks posed by shortsighted legislation (Wiederhold 2022). Furthermore, current cyber law precedents can be adapted to tackle sexual violence in the Metaverse by revising and amending existing laws to incorporate specific provisions for virtual environments (Lee and Min 2022). Laws such as the data protection law and criminal laws addressing sexual offences could be updated to tackle issues of personal information infringement and digital sex crimes within the Metaverse. For example, in the U.K., rape and sexual assaults are defined under the Sexual Offences Act of 2003, but only in real-life situations. This does not extend to the online context or the Metaverse, where offences can have a much worse impact, as previously discussed (Gomez et al. 2024). Likewise, the Act on Special Cases Concerning the Punishment of Sexual Violence Crimes and the Act on the Protection of Children and Juveniles’ Sexuality in South Korea could undergo amendments to offer legal protection against sexual offences in virtual spaces (D. I. Lee 2022).

Drawing on interdisciplinary research into the ethical, psychological, and safety implications of virtual interactions, this study seeks to find a balance among user rights, platform accountability, and the demands of technological advancement. It also considers how cyberlaw precedents addressing issues like cyberbullying and cyberstalking could influence Metaverse-specific regulations (L. Yang 2023). A comprehensive framework, informed by comparative legal analysis and multidisciplinary insights, was developed to address the unique challenges of sexual violence in virtual environments. This article proposes tailored governance strategies based on logical reasoning by integrating comparative findings and extrapolating from technology-specific insights. It offers specific, academically supported policy recommendations for various stakeholders, aiming to create a safer Metaverse for all users.

#### 4. Brief Overview of the Metaverse

The Metaverse, emerging as a potentially groundbreaking development in the technological landscape, is poised to surpass the impact of the Internet. This notion, endorsed by industry leaders, including Facebook's CEO (Newton 2021) and numerous tech experts, underscores the importance of thoroughly understanding the Metaverse's far-reaching implications. Conceptually, the Metaverse represents an expansive virtual domain, its name deriving from the Greek "Meta" (beyond) and "Universe", symbolising a realm that extends beyond our familiar reality. Although defining the Metaverse is challenging, it is generally depicted as a collective, immersive experience in a simulated environment, engaging multiple users in a first-person perspective. This spectrum ranges from complete virtual environments in virtual reality (VR) to augmented reality (AR) integrations within the physical world. AR enhances real-world experiences with virtual components, while VR offers total immersion and is now employed across various sectors, including medical training and virtual social interactions.

In the Metaverse, avatars serve as the digital embodiments of users, facilitating dynamic interactions, exploration, and access to a wide range of digital services. This capability allows users to develop unique identities and personal brands within the virtual landscape.

Creating virtual humans or avatars enables user interactions akin to real-world social dynamics in this environment. However, such interactions carry the potential risks associated with physical interactions, including offences like theft, misrepresentation, fraud, and sexual offences. In the virtual realm, offences such as the unauthorised acquisition of virtual currencies could be equated to virtual theft. Furthermore, the principles of contract law might apply to transactions conducted within this space, introducing concerns about fraud and misrepresentation.

Crucially, interactions between avatars that are sexual in nature also fall under the scrutiny of laws governing sexual conduct. This aspect raises significant legal and ethical considerations, particularly in how existing laws and regulations can be adapted or extended to govern such interactions in the Metaverse. It implies the need for a comprehensive legal framework that addresses the unique challenges posed by virtual environments, ensuring that the rights and safety of users are protected in this emerging digital frontier. This development underscores the importance of understanding the Metaverse not only as a technological innovation but also as a domain requiring careful consideration of legal, ethical, and societal implications.

#### 5. Exploration of Trends—Sexual Crimes in the Metaverse

The emergence of sexual crimes in the Metaverse raises critical questions about the responsibilities of platform developers and operators in monitoring and addressing such behaviours. It also highlights the need for comprehensive legal frameworks and ethical guidelines to combat these issues effectively. This section aims to shed light on the nature of these crimes, their impact on victims, and the broader implications for safety and inclusivity in virtual environments. Understanding and addressing these challenges is essential for ensuring that the Metaverse remains a space that fosters positive and respectful interactions while protecting the rights and well-being of all users.

The Metaverse, designed to replicate real-world social dynamics, facilitates various forms of interaction among avatars, including gaming, virtual tourism, and other recreational activities (Ramirez et al. 2023). While these interactions are intended to enrich the user experience, they also open avenues for both consensual and non-consensual sexual activities. Instances of sexual harassment and assault in the Metaverse are increasingly reported, reflecting a disturbing parallel with real-world trends. Such incidents range from avatars being groped (Belamire 2016) to extreme cases like virtual rape (Sum of US 2021, pp. 5–6). A notable case involved a female researcher's avatar, which was subjected to a simulated rape at a virtual party in view of other avatars (ibid.). In another incident, a user's avatar experienced simulated groping and ejaculation (ibid.). These are not isolated

events but part of a larger pattern of sexual harassment becoming disturbingly frequent in the Metaverse. Research in this domain reveals a further disconcerting trend: minority groups, particularly women, children, and people of colour, are often the primary targets of harassment in virtual environments, mirroring the vulnerabilities these groups face in the physical world (Blackwell et al. 2019). The presence of sexual harassment in the Metaverse exacerbates the risks for already vulnerable groups, particularly children, who are naturally inclined to embrace new technologies such as the Metaverse quickly (Robinson et al. 2020). This inclination, reflective of their inherent digital savviness, brings into sharp focus the grave issue of child sexual exploitation within these virtual spaces.

This deepening concern is intensified by the growing immersion of children and adolescents in digital media, raising serious alarms about the potential negative impacts on their mental and physical health. The Metaverse, in this context, not only amplifies mental health challenges like depression, anxiety, addiction, self-harm, suicidality, and eating disorders but also lays the groundwork for severe social issues. These include cyberbullying, inappropriate sexual behaviour, and exploitation of minors, which are particularly alarming given the already heightened risks of sexual harassment in these environments. Moreover, the Metaverse exposes young users to additional dangers, such as online gambling and significant privacy and security threats (Kim and Kim 2023).

What is particularly disconcerting is the lack of comprehensive research on the societal impacts of the Metaverse, especially at an individual level and in terms of its long-term environmental effects. This lack of research is more than just a gap in academic understanding; it represents a critical oversight in our approach to managing and governing these new digital landscapes. The paucity of focused studies on these issues is a glaring omission, given the potential for profound and lasting effects on our society's most impressionable and vulnerable members. Therefore, developing a more critical and evidence-based understanding of the Metaverse's impact is imperative, ensuring we are not inadvertently placing our younger generations at risk in these uncharted digital territories.

The complexities of the Metaverse further exacerbate these issues. The platform enables adults to disguise themselves as children, potentially deceiving real child users into thinking they are interacting with peers (Lorenzo-Dus and Izura 2017). This deceptive environment poses a significant risk for unsuspecting minors. On the flip side, there is the occurrence of "sexual age-play", where consenting adults use avatars that appear underage (Kierkegaard 2008; Reeves 2013). Though this might not be illegal, it raises ethical concerns and potentially normalises problematic behaviours. These virtual interactions involving the sexual depiction of children create a grey area in both legal and moral terms. The research underscores the seriousness of this issue, indicating that hostile, violent, or abusive experiences in the virtual world can elicit psychological and physiological responses akin to those experienced in the real world (Lee et al. 2021). Thus, the Metaverse not only reflects but potentially intensifies the risks of child sexual exploitation familiar in the real world. This situation underscores the urgency of developing robust safeguards and legal frameworks to protect the most vulnerable users in the Metaverse.

## 6. Unique Challenges: Navigating the Uncharted Terrain of the Metaverse

As we discussed in the previous section, the prevalence of sexual crimes in the Metaverse makes it imperative to delve into the unique challenges this virtual environment presents, especially in the context of these offences. The Metaverse, a burgeoning and evolving digital realm, brings forth complexities not typically seen in the physical world, necessitating a nuanced understanding and approach.

A primary challenge in the Metaverse is the ambiguity surrounding consent. Unlike in the physical world, where the norms and boundaries of consent are more clearly defined and understood, these boundaries become blurred in the Metaverse. The virtual nature of interactions complicates the understanding of consent, as communication nuances and intentions can be misinterpreted or lost in digital translation. This is further complicated by the potential for user misrepresentation and the inherent anonymity within these spaces.

Such factors can lead to scenarios where actions, including unsolicited advances, may not be uniformly perceived as inappropriate by all parties involved, potentially leading to instances of sexual violence. Anonymity in the Metaverse also presents a significant challenge. While it gives users a sense of freedom and privacy, it can simultaneously encourage them to engage in behaviours they might otherwise avoid in the real world. This sense of detachment, combined with perceived impunity, can escalate the frequency and severity of sexual violence in these virtual spaces. Striking a balance between the benefits of anonymity and the need to deter harmful behaviours becomes critical to managing these environments.<sup>1</sup>

Furthermore, the psychological impact of experiences in the Metaverse, particularly those related to sexual violence, is a crucial factor. Even though these experiences are virtual, they can have tangible psychological effects on victims, including trauma, fear, and distress, mirroring the impacts of real-world sexual violence. Thus, addressing the unique challenges of the Metaverse, especially in the context of sexual violence, requires a multifaceted strategy. This strategy should encompass technological solutions, community guidelines, legal adaptations, and psychological support mechanisms. The development of robust legal frameworks that can adapt to the intricacies of virtual environments is particularly urgent.

### 6.1. Virtual Consent

Exploring the intricate issue of virtual consent within the Metaverse, it is crucial to understand how it diverges from traditional notions of consent in the physical world. Factors such as avatar autonomy, the blurred distinction between player and character, and potential miscommunication in digital interactions significantly impact how consent is perceived and negotiated in virtual spaces. A study by Zytko and Chan sheds light on the alarming absence of consent mechanisms in virtual societies (Zytko and Chan 2023). Zytko and Chan point out that social Virtual Reality (VR) environment developers often overlook the need for consent-based frameworks. This negligence contributes to and exacerbates the occurrence of criminal sexual offences in these virtual realms. The absence of a system for explicitly exchanging consent allows for and indirectly encourages situations that lead to such offences.

In VR, participants engage in sexual exploration through their avatars, leading to overtly sexual experiences. These experiences can range from erotic body movements and promiscuous verbal dialogue to non-consensual interactions, sometimes involving underage users. The complexity of eliminating sexual violence or harmful behaviour in the Metaverse is underscored. Participants in Zytko and Chan's study found themselves in a grey area regarding what constitutes sexually appropriate behaviour in virtual spaces (Zytko and Chan 2023). This ambiguity largely stems from the absence of a clear, qualitative standard for assessing behaviour, resulting in varied perceptions and responses to sexual interactions. Establishing mechanisms that address these issues is essential for safeguarding users in the Metaverse. Without such mechanisms, users are vulnerable to harmful behaviours that blur the lines between virtual and real-world consequences.

#### 6.1.1. Avatar Autonomy and Blurred Lines between Player and Character

In the Metaverse, where users adopt avatars for interaction, the concept of embodiment creates a profound connection between users and their virtual representations (Gonzalez-Franco et al. 2020). This phenomenon holds both promising and problematic potential. Positively, it allows individuals to transcend their real-life limitations, creating idealised versions of themselves (King et al. 2020). However, this can inadvertently set unrealistic beauty and lifestyle standards, fostering unhealthy comparisons and possibly aggravating issues like body dysmorphia, especially among younger users who are at a crucial stage of identity development (Abbas and Dodeen 2022).

---

<sup>1</sup> We will discuss this later on in the paper.

As discussed before, virtual consent and bodily autonomy become particularly complex in the Metaverse. Instances of sexual harassment, such as the non-consensual touching of an avatar, challenge our understanding of consent in these digital realms. While such actions are unequivocally deemed sexual harassment in the real world, the translation of these norms to virtual avatars is not straightforward. The ambiguity lies in whether the autonomy and rights afforded to a person's physical self should extend equally to their digital avatar (Freeman et al. 2022). In real-world social interactions, there are established norms regarding physical proximity, where unwanted closeness is recognised as harassment (ibid.). Scholars argue for a parallel in virtual environments: actions that invade personal space without consent, even in a digital context, should be seen as potential harassment (ibid.). This perspective suggests that avatars in the Metaverse are more than mere digital entities; they are extensions of the users' personal autonomy (ibid.). Therefore, the actions and choices made by these avatars could reflect the users' intentions and deserve respect and legal consideration similar to those in the physical world.

These factors complicate the application of criminal liability to virtual experiences. While users can theoretically disengage at any time, the phenomenon of involuntary paralysis or "tonic immobility" during traumatic experiences raises questions about the user's ability to exercise this control (Kalaf et al. 2017). Research is needed to determine whether sexual crimes in the Metaverse can evoke tonic immobility and, if so, whether its degree is comparable to real-world experiences. Without concrete answers, uncertainty remains about how much an avatar represents the end user and the degree of autonomy and agency a user possesses in exercising consent in virtual environments. This uncertainty underscores the need for a nuanced understanding of consent and autonomy in the Metaverse.

#### 6.1.2. Potential for Miscommunication

The Metaverse, transcending geographical and cultural boundaries, hosts a diverse global user base, each with unique social and moral norms. This diversity, while enriching, inevitably leads to communication challenges. Users from different regions and backgrounds may unintentionally offend each other's sentiments because of these varying norms. Often resulting from these cultural disparities, miscommunication can lead to unintended and sometimes undesirable outcomes. However, it is essential to recognise that users are not entirely naive in their approach to cross-cultural communication. Current social media platforms serve a global audience and operate under certain 'community standards' that guide user interactions. Users from diverse backgrounds generally respect these standards, each socialised in different environments.

Similarly, issues like sexual abuse and violence tend to garner a broad consensus across various communities, suggesting the possibility of establishing universal community standards in the Metaverse. Despite this, subtler issues may arise in the Metaverse, particularly around softer or more nuanced remarks. What might be considered sexually offensive can vary significantly depending on a user's societal upbringing and understanding of social norms. These nuances present challenges in establishing a one-size-fits-all standard for communication and behaviour.

The Metaverse, offering immersive real-life simulations, intensifies these challenges beyond the traditional text and image-based interactions of the current Internet. In such a highly interactive and realistic environment, the potential for miscommunication and misunderstanding is not only present but could be significantly amplified. Navigating this complexity requires a nuanced approach to community standards, one that is sensitive to the diverse backgrounds of users and adaptable to the unique communicative dynamics of the Metaverse. This approach is essential for fostering a respectful, inclusive, and safe environment for all users, regardless of their cultural or geographical origins.

#### 6.2. Impact of Anonymity

The impact of anonymity in the Metaverse is a critical issue, particularly when considering its influence on incidents of sexual violence. This anonymity, inherent to the

Metaverse's virtual realms, allows users to interact without revealing their true identities, which can encourage damaging behaviours. This aspect of facelessness in the Metaverse is not merely a feature; it represents a complex challenge that amplifies the difficulties in supporting victims and identifying perpetrators. In the Metaverse, the challenge of identifying the real individual behind an avatar is substantial. The creation and customisation of avatars are subject to minimal restrictions, making it nearly impossible to ascertain the true identity of a user (Jesse 2019–2020). This flexibility allows individuals to disguise their identity completely, even assuming entirely false personas. For instance, in platforms where avatars are meant to represent the user's real appearance, it is easy for individuals to create deceptive avatars using someone else's photo, further complicating the authenticity issue (Lin and Latoschik 2022).

Taking "Second Life" as an illustrative example, the platform allows users to choose their avatars' first names, permitting using abstract or non-descriptive names. This policy promotes creativity and freedom but also facilitates a high degree of anonymity. Similarly, the lack of verification mechanisms compromises the platform's age restriction policy, enforced through a birthdate requirement. Users often create new, separate email accounts specifically for such platforms, further obscuring their real-world identities. In addition, avatar customisation in the Metaverse, which includes modifications to physical appearance and attire, complicates the identification of a user's actual gender and age. While platform owners may identify which account created an avatar, to other users, these avatars function essentially as pseudonyms. However, the anonymity afforded by these avatars is undermined as they develop sub-identities within the Metaverse. These sub-identities, shaped by behavioural patterns and shared knowledge, can inadvertently reveal personal information about the user, thereby compromising their privacy.

The various layers of anonymity in the Metaverse present significant challenges in criminal situations, particularly in identifying perpetrators. This environment also creates opportunities for malicious activities, such as creating fake avatars to impersonate others or commit crimes in their name. The complexity of these issues demands a nuanced approach to identity management in the Metaverse. Ensuring accountability and safety while preserving the freedom of expression requires a delicate balance and potentially innovative technological and regulatory solutions. This balance is crucial for maintaining the integrity of interactions within the Metaverse and protecting users from harm.

### *6.3. Detrimental Psychological Effects*

We examine the potential psychological effects of sexual violence within the Metaverse in this section. Drawing on insights from cyberpsychology, we aim to understand the harmful impacts these occurrences can have on a user's mental well-being, potentially causing trauma similar to that experienced by victims of sexual violence in the real world. The Metaverse presents various forms of virtual worlds, each with distinct implications for how users relate to their avatars. In some of these worlds, users are limited to using standardised avatars with little to no opportunity for customisation. In such environments, the degree of emotional attachment or identification a user feels towards their avatar might be minimal because of the lack of expression of personal identity. This diminished attachment could result in a reduced psychological impact from any experiences of virtual abuse or harassment. On the other hand, there are virtual spaces that allow users extensive customisation options for their avatars. Users can craft unique identities in these settings that reflect their personal characteristics and preferences. Such a deep level of personalisation can lead to a stronger emotional bond with the avatar, making experiences of sexual violence in these contexts potentially more traumatic. Users might perceive these violations as direct attacks on self-representation, leading to significant emotional distress. The psychological effects of these two types of virtual environments are markedly different. Where avatars are standardised and impersonal, users may experience a certain degree of detachment from negative experiences, mitigating the psychological impact. However, in environments with highly personalised avatars, the repercussions of sexual violence can be as severe as those

experienced in the physical world, including feelings of fear, anxiety, and psychological distress.

This variation in psychological impacts highlights the importance of understanding the complex dynamics of user–avatar relationships in the Metaverse. As virtual environments evolve to offer more personalised experiences, the potential for psychological harm escalates, underscoring the need for measures to safeguard users' mental health. Such measures could include establishing support systems for victims, implementing community guidelines to prevent abuse, and educating users about the risks and ethical responsibilities of virtual interactions. Addressing these psychological dimensions is vital for maintaining the Metaverse as a safe, inclusive, and respectful digital landscape (Freeman et al. 2022).

This perception engenders a sense of responsibility and protectiveness towards the avatar, reflecting the user's role and identity within the virtual world (ibid.). Emerging research in this field indicates that the more the virtual world resembles the real world, the more likely it is for the user's brain to process virtual experiences similarly to real-life experiences. This phenomenon is not just about visual and aesthetic similarity; it is also about the immersive quality of the experience. Modern virtual reality hardware is crucial in enhancing this sense of immersion.

Devices such as VR headsets and haptic gloves create a compelling sense of "presence", making the virtual experience more real and immediate.<sup>2</sup> This refers to the experience of "being inside" the simulated environment, i.e., successful "location" illusion (Cummings and Bailenson 2016), and the feeling that one is performing some action (even though the setting is virtual), i.e., the "action" illusion because of this, a so-called "virtually real experience" is created, i.e., an experience perceived to be "real at the moment of experience" (Montefiore and Formosa 2022; Ramirez 2022). For example, in an interview, VR researcher Jessica Outlaw states that when talking to people she knows in a VR headset, she feels she is with them, has an embodied experience, and "creates memories" with them (Dolan 2022). Research also suggests that in a Metaverse setting, the neural response of the brain remains the same as that in the physical world. Hence, in a realistic game setting, a user might feel scared to death if their avatar is in a near-death situation, even though no actual physical harm ever occurred to the user (Lemley and Volokh 2018). Cyber violence has been found to cause psychological harm such as depression, stress, anxiety and post-traumatic stress disorder (Cripps and Stermac 2018). Therefore, the psychological impact in the Metaverse is more significant and much different than a typical online scenario such as a simple video game (Lemley and Volokh 2018). It may be said to be close to a real-world impact since it triggers responses similar to those in the real world.

## 7. Existing Legal Frameworks

This section aims to critically examine the adequacy of current legal frameworks in addressing sexual violence within both traditional physical settings and emerging digital platforms, with a specific focus on the Metaverse. Our analysis is grounded in an extensive review of the legal systems in the United States, the European Union, and South Korea, complemented by relevant case studies that shed light on the practical application of these laws. The legal systems in these regions have evolved to address sexual violence, primarily in physical contexts. However, the transition to digital spaces, notably the Metaverse, raises complex legal questions. The central challenge is adapting laws crafted for tangible interactions to the virtual realm, where the dynamics of sexual violence can be vastly different, blurring the lines between physical and psychological harm.

In the United States, existing laws on sexual harassment and assault are predominantly oriented towards physical incidents. The rise of digital harassment has led some states to expand their legal frameworks to encompass online forms of these crimes. However, the immersive and interactive nature of the Metaverse, where experiences of sexual violence

<sup>2</sup> Dolan (2022, p. 44) (also refer to the example of Project Cambria, which imitates real-world virtual social settings).

can have profound psychological impacts, pushes the boundaries of these legal adaptations. The European Union's approach to harassment and online abuse demonstrates a recognition of the evolving nature of sexual violence in digital spaces. Despite comprehensive laws against harassment, the unique challenges of virtual environments, such as jurisdictional issues in a borderless virtual world and the difficulty in pinpointing perpetrators behind anonymous avatars, pose significant hurdles to effective legal application in the Metaverse. South Korea's experience is particularly instructive, given its advanced digital culture and specific legislation targeting cybercrimes. Even here, the legal framework is in a continuous state of flux, striving to keep pace with the nuances of digital interaction, especially in an immersive environment like the Metaverse.

These jurisdictional insights reveal a shared predicament: while existing legal frameworks lay a foundational structure for addressing sexual violence, they fall short of fully encompassing the complexities presented by the Metaverse. The challenges are multifaceted, encompassing the definition and scope of sexual violence in virtual spaces, the identification and prosecution of perpetrators who may exploit anonymity, and providing adequate support and justice for victims. This situation underscores an urgent need for legal systems to evolve and adapt, ensuring robust protection and redressal mechanisms for users navigating the digital terrain of the Metaverse.

### 7.1. United States

Exploring the legal landscape of the United States, we focus on the application and potential limitations of existing laws regarding sexual violence, specifically in the context of the Metaverse. Our analysis draws connections to the earlier discussions in this paper, examining how the U.S. legal system addresses sexual offences in both physical and increasingly prevalent digital spaces like the Metaverse. The Child Pornography Prevention Act of 1996 (CPPA) marked the U.S.'s initial legislative foray into curbing virtual child pornography.<sup>3</sup> This legislation included provisions for penalising depictions of minors, or images that "appeared to be" minors, in sexually explicit conduct, including computer-generated representations.<sup>4</sup> This broad definition held potential relevance for the Metaverse, particularly for combating sexual depictions of children using virtual or morphed images. However, in *Ashcroft v Free Speech Coalition*,<sup>5</sup> the Supreme Court struck down these provisions as unconstitutional, citing an overly broad interpretation that infringed upon free speech rights by prohibiting representations that did not involve actual children.<sup>6</sup> The Court refused to accept that they should be prohibited because depictions may tend to encourage child abuse in the real world. It stated that "*the mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it*".<sup>7</sup> The provision was found to violate the right of free speech guaranteed by the First Amendment.<sup>8</sup>

In response, the U.S. implemented the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act in 2003. This law, while narrower than CPPA, included "indistinguishable" computer images of minors or images modified to resemble identifiable minors.<sup>9</sup> This definition's applicability to the Metaverse is critical, particularly for instances where avatars of minors are used or altered for sexually explicit purposes. However, the Act's effectiveness in addressing the nuanced realities of

<sup>3</sup> Section 121(2), Child Pornography Prevention Act 1996.

<sup>4</sup> See Footnote 3.

<sup>5</sup> *Ashcroft v Free Speech Coalition* 535 U.S. 234 (2002) ('*Ashcroft*'). <https://supreme.justia.com/cases/federal/us/535/234/> Accessed on 16 February 2024.

<sup>6</sup> *Ashcroft v Free Speech Coalition* 535 U.S. 234 (2002) ('*Ashcroft*'). <https://supreme.justia.com/cases/federal/us/535/234/> Accessed on 16 February 2023.

<sup>7</sup> *Ashcroft v Free Speech Coalition* 535 U.S. 234 (2002) ('*Ashcroft*'), p. 253.

<sup>8</sup> *Ashcroft v Free Speech Coalition* 535 U.S. 234 (2002) ('*Ashcroft*'), p. 244.

<sup>9</sup> Child pornography is defined as any visual depiction of sexually explicit conduct that includes the following: (a) a minor, (b) a digital or computer image that is "indistinguishable" from that of a real minor, or (c) an image which has been created or modified to appear to be that of an "identifiable minor" engaging in sexually explicit conduct (18 U.S.C. § 2256(8)).

sexual violence in the Metaverse remains an open question, highlighting the need for legal frameworks that can adapt to the complex dynamics of virtual environments.

State-level laws in the U.S. also address virtual sexual conduct, but they face challenges balancing regulation with freedom of speech, a deeply entrenched value in American jurisprudence. The high threshold for penalisation in cases like those under California Penal Code Section 653.2 illustrates the difficulty in proving intent in virtual interactions within the Metaverse.<sup>10</sup> However, to prove the same, it is necessary to satisfy that the messages were sent with the purpose of “*imminently causing that other person unwanted physical contact, injury, or harassment*”.<sup>11</sup> Establishing unwanted physical contact, injury, or harassment in interactions that happen in the Metaverse would be challenging.

Section 230 of the Communications Decency Act (CDA) further complicates the issue of accountability in the Metaverse. This clause effectively absolves Metaverse platforms from responsibility for user-generated content by exempting service providers from liability for third-party content. This lack of liability raises critical questions about the role of these platforms in moderating and preventing sexual violence within their virtual spaces. Clause (c)(2) states that “*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*”.<sup>12</sup> By not being considered publishers, service providers are immune from any claim against content posted by users. Although no case has come up, it is fair to assume that Metaverse platforms, being interactive computer services, will enjoy the same immunity as any other service provider under Section 230.

The juxtaposition of these legal frameworks with the emerging challenges posed by the Metaverse underscores a significant gap. The U.S. legal system, while providing a foundation for addressing sexual violence, falls short in effectively tackling the unique issues presented by virtual environments. There is a pressing need for legal evolution that considers the Metaverse’s immersive and interactive nature, ensuring adequate user protection and holding perpetrators accountable in these digital realms. This situation calls for a critical re-evaluation of existing laws and potentially the development of new legal standards that are better equipped to address the complexities of sexual violence in the Metaverse.

## 7.2. European Union

Examining the European Union’s (EU)’s legal framework reveals that, like many other jurisdictions, no specific legislation is tailored to the Metaverse. This absence reflects the broader challenge of legislating for such expansive and multifaceted digital spaces. The Metaverse’s complex and evolving nature makes the concept of a single, comprehensive “Metaverse law” as elusive as the notion of a singular “Internet law”.

Given the Metaverse’s complex nature, the EU approach appears to target specific areas of concern rather than attempting to create an overarching “Metaverse law”. Key focus areas include competition, data protection, and intellectual property. Each of these domains presents unique challenges in the context of the Metaverse. For instance, issues of competition involve how virtual platforms interact, the monopolisation of virtual spaces, and the fair usage of virtual marketplaces. Data protection becomes increasingly complex in an environment where personal and behavioural data can be collected on a much more intricate level than on conventional Internet platforms. Intellectual property concerns in the Metaverse revolve around using and misusing digital assets, ranging from virtual goods to unique user-created content (EPRS 2022).

Certain aspects of the current framework might assist in dealing with sexual harassment cases in the Metaverse. The definition of “child pornography” according to the *Council of Europe Convention on Cybercrime* is “realistic images representing a minor en-

<sup>10</sup> S. 653.2 of the California Penal Code.

<sup>11</sup> See Footnote 10.

<sup>12</sup> Section 230(c)(2), Communications Decency Act, 1996.

gaged in sexually explicit conduct". A similar and further expanded definition of "child pornography" exists under the EU Directive on *Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography*, wherein the term includes "realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes". These definitions are broad since they include "realistic images" instead of only actual ones. This allows the potential inclusion of virtual representations and pornography in the Metaverse into their domain.

Apart from this, the EU has also looked into intermediaries' liabilities regarding the content they host online. However, currently, any stringent and exhaustive law that encapsulates all the aspects relating to sexual crimes occurring in the Metaverse does not exist in the EU legal framework, but steps have been taken to address this omission. In April 2022, the EU agreed upon the *Digital Services Act* ("DSA"), legislation addressing illegal and harmful Internet content.<sup>13</sup> Focusing on intermediaries, the law puts the onus of monitoring hosted content on the tech company or facing a fine of up to 6 per cent of the global revenue. The obligations have been made proportionate to the size of the tech company based on the nature of services offered and the number of users (European Council 2022). Large online platforms, or VLOPs, have been subject to more stringent requirements. These platforms will be required to analyse the systemic risks they create and conduct risk reduction analysis (ibid.). Areas of risk that have been identified include effects on fundamental rights, gender-based violence, effects on the physical and mental health of users, and impact on minors, amongst others (ibid.). While the exact application of the DSA cannot be observed until its implementation, it has the potential to be applied to Metaverse platforms. As the popularity of such platforms increases in the coming years, these platforms will eventually become VLOPs because of an increase in the user base. Another reason for them to become VLOPs could be the upcoming trend in many essential services offered in the Metaverse. Many big corporations have opened virtual stores and office spaces in the Metaverse. As this wave continues, the services these platforms provide will become diverse and gain more traction. The increased social interaction in a world that simulates reality would possess risks on counts of sexual harassment, verbal abuse, and fraud. Legislation such as the DSA would ensure the platforms realise their accountability, continuously analyse the content being circulated, and devise risk reduction mechanisms.

### 7.3. United Kingdom

The United Kingdom's introduction of the Online Safety Act 2023 represents a significant stride in digital regulation, particularly relevant to emerging virtual environments like the Metaverse. This legislation, focusing on enhancing online safety and specifically targeting child sexual abuse, necessitates a nuanced examination of its potential impact on the complex dynamics of the Metaverse. The legislation delegates new powers and responsibilities to OFCOM, setting a precedent for a stringent approach against child sexual abuse in digital spaces. This proactive stance is vital for the Metaverse, a domain where the immersive nature of interactions amplifies the potential for harassment, sexual abuse, and bullying. However, applying this law to the Metaverse, which is a more intricate digital space than traditional online platforms, presents unique challenges.

One area of contention within the legislation is its handling of misinformation. This aspect has sparked significant debate, reflecting the delicate balance between regulating harmful content and preserving free speech. The Metaverse, with its rich user-generated content and diverse modes of expression, complicates this balance further. Differentiating between harmful misinformation and legitimate expression within such a multifaceted virtual world is a challenge the law must navigate carefully.

The legislation's implementation strategy, placing substantial responsibility on tech companies, is crucial but also demanding. These firms are expected to revolutionise their safety governance, align service design with safety priorities, and enhance user autonomy

<sup>13</sup> The Act is still subject to formal approval as of June 2023.

over online experiences. While these expectations are commendable, their translation into the context of the Metaverse, characterised by rapidly evolving technologies and user interactions, is complex. The effectiveness of these measures in a virtual environment that blurs the lines between reality and digital representation is yet to be fully understood.

Furthermore, the law-phased approach, encompassing regulating illegal content, child safety, and user empowerment, suggests a methodical regulatory process. However, the effectiveness of this approach within the Metaverse, where user interactions are multifaceted, and the nature of the content is continually evolving, is an area that requires careful consideration. The requirement for online platforms to publish transparency reports is a step towards greater accountability, but applying this to the diverse and dynamic world of the Metaverse poses its own set of challenges.

The Online Safety Act's provision for substantial fines underscores OFCOM's strong enforcement stance. Nonetheless, ensuring adherence across the board, especially for smaller companies with limited resources, and keeping up with the fast-paced evolution of the Metaverse are daunting tasks. The adaptability and responsiveness to the unique challenges of the Metaverse will be critical to its success. Striking the right balance between safeguarding users, particularly children, and upholding the rights and freedoms of all participants in the Metaverse is pivotal for the effective regulation of this burgeoning digital frontier.

#### 7.4. South Korea

There is a growing concern in South Korea that Metaverse interactions are becoming hotspots for sexual harassment of minors. Metaverse harassment is becoming common, and sexual slurs are easily evident in waiting areas such as game rooms (Forkast 2022b). Cases have come up where adults are inducing minors with gifts in the Metaverse to solicit sexually explicit photos (ibid.). Because of such incidents, there is a demand to create a separate regulatory framework explicitly dealing with the Metaverse. Current laws are inadequate to address issues in the virtual world, as they are limited to the actual physical harassment of humans. Even in the digital world, sexual violence or abuse of a verbal nature is deemed criminal only when it occurs in a public space.<sup>14</sup> Consequently, any abusive messages being sent in private chats in the Metaverse would not draw punishment.<sup>15</sup>

The limitations of the current framework are being recognised, and new amendments to the existing Youth Protection Law are being forwarded, aiming to increase the accountability of online platform operators (Bill Information 2022). A Council was created in 2022 by the country's media regulation agency, the Korea Communications Commission, to brainstorm the regulatory framework for building a trusting, ethical, and fair Metaverse (Forkast 2022a). It comprises 30 professionals from different fields, such as law, media, technology, and industrial management. Additionally, the Ministry of Science and ICT ("MSIT") released non-binding ethics guidelines for the Metaverse, called "Ethical Principles for the Metaverse" (MSIT). The expectation is for the document to serve as a code of conduct for users and Metaverse platforms. The guidelines focus on three main values including sincere identity, safe experience, and sustainable prosperity (ibid.). Under these, principles such as authenticity, autonomy, privacy, and protection of personal information are at focus (ibid.). Addressing privacy, the guidelines recognise that the Metaverse creates a sense of immersion and allows the real self to connect to the virtual self through sight, hearing, and other purposes.<sup>16</sup> Users are advised to be cognisant of their virtual movements so as not to infringe upon the privacy of others (ibid.). Developers and operators are advised to provide methods to users that allow them to respond quickly should their private areas be infringed (ibid.).

<sup>14</sup> Seo Ji-hyun, head of the Ministry of Justice's digital sex crime task force, revealed at a recent debate (the exact source of this could not be located. It appears that there is no documented record of the event available publicly, so the news report is the only source for this).

<sup>15</sup> See Footnote 14.

<sup>16</sup> MSIT (under Practical Principle 4: Respect for Privacy).

South Korea embarked on its cybersecurity journey during the late 1980s when the government promoted the increased dissemination of information. In the private sector, various agencies devised strategies, but these were primarily limited to their own domains, needing more comprehensive, nationwide coordination. Practical countermeasures mainly targeted individual malicious activities. However, as cybercrimes proliferated exponentially, the government recognised the need for a more comprehensive approach. Attempts were made towards the end of the first decade of the 21st century. Still, instead of developing robust strategies and mandating online protection across platforms, the focus remained on policy development. The existing regulations concerning the Metaverse are not government-mandated but implemented by individual platforms themselves. For example, South Korean games like *Overwatch* require players to register using their citizen identification number. This has the potential to identify players who harass other users.

As far as the current laws are concerned, some acts can cursorily be applied to the Metaverse until a sound legal regime is built. The Act on Special Cases Concerning the Punishment of Sexual Crimes includes Article 13, which deals with “Obscene Acts by Using Medium of Communications”. Under this article, a person can be punished if it is shown that they have sent “another person any words, sounds, writings, pictures, images or other things, which may cause a sense of sexual shame or aversion, through telephone, mail, computer or other means of communication, with intent to arouse or satisfy his/her own or the other person’s sexual urges”.<sup>17</sup> Even if this provision were to be applied in Metaverse situations, problems would arise concerning the identification of the user behind avatars. Since avatars are often customisable, lifting the veil of anonymity and identifying the perpetrator is difficult.

Besides this, the law on the Protection of Children and Juveniles from Sexual Abuse deals specifically with minors. In its definition of “child or juvenile pornography”, the law includes a depiction of children or juveniles doing acts of a sexual nature in the form of video, game software, and pictures. Per Article 8(5) of the Act, recruiting a child to produce pornography, knowing that it is intended for pornographic use, is punishable. It can be argued that in a game within the Metaverse, if one user lures a minor into engaging in a sexual act to produce a recording, it could be considered the production of child pornography and be punishable. Because of the inclusion of game software in the definition of child pornography, such instances of abuse in virtual games may be covered. However, this is still speculative and, even if accepted, would not address other acts in the Metaverse that can constitute sexual harassment.

South Korea has also sought international collaboration to bolster online platform security and tackle online threats. Despite a good understanding of online harms, research on the associated legal aspects still needs to be conducted. While some technological solutions have been explored, a more comprehensive and institutionalised policy framework is essential to ensure the effective nationwide implementation of any such solution (Kim and Bae 2021).

## 8. Bridging the Gap: Proposals for a Legal Framework

In light of the analyses conducted on the current legal frameworks and their applicability to the Metaverse, a discernible gap in regulation is evident. This gap necessitates a dedicated and nuanced legal approach tailored specifically to address the unique challenges posed by virtual environments. This discussion puts forth a series of legislative recommendations and guidelines carefully designed to pioneer an effective regulatory framework for the Metaverse. A critical aspect of this proposed framework is the redefinition and understanding of consent within virtual spaces. Traditional legal definitions of consent do not adequately encapsulate the complexities inherent in the Metaverse. Thus, there is a need to develop a distinct protocol for virtual interactions that ensures explicit consent is obtained and respected in a contextually relevant manner to the Metaverse.

<sup>17</sup> Translation from the actual text as provided by Korea Legislation Research Institute ([https://elaw.klri.re.kr/eng\\_service/lawView.do?hseq=40947&lang=ENG](https://elaw.klri.re.kr/eng_service/lawView.do?hseq=40947&lang=ENG)). Accessed on 16 February 2024.

The global and borderless nature of the Metaverse introduces significant jurisdictional challenges. Addressing these requires an innovative approach, potentially in the form of an international legal treaty or framework. Such a framework should facilitate cross-border cooperation for investigating and prosecuting offences within the Metaverse, ensuring no perpetrator evades accountability because of geographical limitations. Moreover, the challenges posed by the anonymity of users and the transient nature of digital interactions in the Metaverse make enforcement particularly daunting. A balanced approach to digital identity verification is imperative, one that harmonises the privacy of users with the necessity for accountability. Additionally, a legal mandate should be put in place to preserve digital interactions within the Metaverse, akin to financial transaction logs, to support investigative and judicial processes.

The role of Metaverse platforms as service providers is also a focal point. Under the new legal framework, these platforms should be obligated to implement comprehensive moderation systems, conduct user verification processes, and monitor content effectively. This approach aligns with the responsibilities outlined in legislation such as the U.K.'s Online Safety Act, setting a precedent for platform accountability in preventing and addressing abuses within their virtual environments. Finally, user empowerment within the Metaverse is paramount. Legal mechanisms must be established to facilitate easy reporting of abuses, access to support and assistance, and tools for users to manage their digital environment. An accessible and transparent process for reporting violations and seeking redress should be integral to the regulatory framework.

#### *8.1. Novel Legal Definitions of Virtual Harm*

In the Metaverse, the convergence of virtual and physical realities presents a unique challenge in distinguishing between harm inflicted in these two spheres. The rapid adoption of advanced technologies in this interactive online space has made it increasingly possible to cause harm in virtual settings. This notion of virtual harm extends beyond mere tangible damage; it encompasses the psychological distress resulting from manipulation, harassment, and online bullying that occur within these digital environments.

The current legal frameworks, however, often fall short of addressing the full spectrum of harm that can be perpetrated in the Metaverse. Therefore, there is a pressing need to broaden the legal definition of virtual harm. This expansion must go beyond the traditional understanding of harm to include virtual representations of illegal content, such as child pornography or sexually explicit conduct. It is essential to recognise that these virtual depictions, while not occurring in a physical space, can have severe psychological impacts on individuals, potentially leading to devastating consequences. A more comprehensive definition of virtual harm should encompass the direct effects of such content on victims and the broader societal impact. For example, virtual depictions of child pornography in the Metaverse, even if not involving real children, can contribute to the normalisation of such behaviour and pose significant risks to public morals and individual well-being. Similarly, virtual sexual harassment, while lacking physical contact, can cause psychological trauma comparable to its physical counterpart.

In redefining virtual harm, it is crucial to consider the unique characteristics of the Metaverse, where users often have a heightened sense of presence and emotional investment in their virtual avatars. As such, the psychological impact of harm in these spaces can be profound, necessitating legal protections as robust as those in the physical world. This expanded legal understanding of virtual harm would necessitate novel regulatory mechanisms to protect individuals in the Metaverse. These mechanisms must be capable of addressing the complexities of virtual harm, balancing the need to protect users with the inherent freedoms of digital spaces. It calls for a nuanced approach that acknowledges the evolving nature of harm in an increasingly digitised world and the need for adaptable and responsive laws.

## 8.2. Incorporating Consent Mechanisms

Effective consent mechanisms are paramount in the Metaverse to ensure respectful and safe interactions among users. These mechanisms should begin with the fundamental process of sensitising users to the unique dynamics of this new technological environment. As users navigate the Metaverse, an awareness of the norms and etiquette essential for harmonious co-existence is crucial. To this end, platforms could implement mandatory tutorials for new users and those against whom complaints have been lodged to educate them on the expected standards of behaviour. A key aspect of these tutorials should be the establishment of “clear and in-word” exchange mechanisms for obtaining affirmative consent among avatars. This could involve explicit and easily understandable prompts or agreements before any interaction is construed as invasive or personal. Such a mechanism ensures that all parties involved in an interaction have explicitly agreed to the terms of engagement, thereby reducing the likelihood of misunderstandings or non-consensual encounters. Additionally, users should have the ability to define and control their level of participation in various settings within the Metaverse. This means providing users with tools to set personal boundaries and control how other avatars interact.

An example of this is Meta’s implementation of the “Personal Boundary” feature. This feature creates a virtual 4-foot safety bubble around an avatar, effectively preventing close contact and reducing the chances of harassment. Such features empower users to take active control of their virtual space, contributing to a safer and more respectful virtual environment. Incorporating these consent mechanisms is a step towards creating a safer Metaverse and an essential move in educating users about the importance of consent in digital interactions.

As the Metaverse continues to evolve, these mechanisms need to be adaptable and responsive to new challenges and user needs. Continuous evaluation and improvement of consent practices will be essential in maintaining a respectful and secure virtual environment for all users (Sharma 2022). Other kinds of interaction techniques, such as the ability to blur one’s avatar in an uncomfortable setting, might be useful (Lin and Latoschik 2022). Users may also be given the ability to switch the rendering of their avatar (e.g., cartoon-like depiction, silhouette depiction, realistic depiction) (Volante et al. 2016) depending on what they feel would be most comfortable for them in a situation. This would allow them to participate in a personalised manner while having the ability to hide identifiable details (Lin and Latoschik 2022).

Users in the Metaverse should have effective tools to manage interactions, such as controlling the visibility of other avatars and “red button” functions to remove users from personal virtual spaces immediately. Implementing these features is crucial in reducing unwanted interactions and preventing harassment. Metaverse platforms must integrate diverse and accessible safety measures, including automated personal distance restrictions akin to a “Safe Zone”, universal alarm gestures, and comprehensive tutorials on community guidelines, supplemented by active moderation. Ideally, a combination of these strategies would be employed to maximise safety. However, addressing harassment extends beyond individual platform measures to involve government regulation in content moderation, where current laws remain underdeveloped, particularly those protecting against sexual harassment in virtual environments. Legal frameworks concerning digital avatars are also developing. The Metaverse, as an emerging frontier for online interaction, introduces unique challenges that existing legislation has not comprehensively addressed. Creating safer online environments necessitates a multifaceted approach that includes collaboration among corporations, non-governmental organisations, and government bodies. These stakeholders can establish industry standards and best practices for safer technology use by working together. This collective effort is vital for ensuring user safety and must adapt continuously to the evolving challenges presented by technological advancements like the Metaverse. A combination of platform-based safety features, broader regulatory measures, and industry-wide collaboration can forge a more secure and respectful virtual environment for all users (Wiederhold 2022).

### *8.3. Establishing Special Jurisdictional Rules*

The Metaverse's inherently global nature presents significant jurisdictional challenges in resolving disputes. The overlap of national laws can lead to competing jurisdictional claims, complicating the legal landscape. A pertinent example is the General Data Protection Regulation (GDPR) of the European Union (EU). Under GDPR, a non-EU-based website development company monitoring and analysing data from EU citizens is subject to its provisions, regardless of the company's location. This scenario illustrates how a U.S.-based Metaverse platform serving EU citizens might be subject to jurisdictional claims under U.S. and EU laws, complicating the determination of the applicable legal forum and laws in Metaverse-related cases.

Given the absence of a universally accepted jurisdiction for digital realms like the Metaverse, international cooperation is essential. Countries could work towards a consensus on a legal framework addressing critical issues such as consent, user anonymity, and financial transactions in the Metaverse. The United Kingdom's dedicated jurisdiction for online safety, as outlined in its Online Safety Act, provides an instructive model for other nations. However, the multifaceted nature of the Internet, which operates without regard for national borders, makes the establishment of a singular, definitive jurisdiction challenging, especially in the context of AI and virtual environments.

This complexity necessitates a collaborative international effort to address online safety as a collective responsibility. While a virtual jurisdiction system governed by a specific legal body dedicated to Metaverse offences is innovative, its feasibility is subject to scepticism. It may be overly optimistic to expect states to relinquish jurisdiction over their citizens or to trust an external entity with such authority. A more practical approach might involve creating a legal body within an international organisation tasked with overseeing and issuing standardised rules and regulations for states to implement. This body could help smooth out jurisdictional overlaps, ensuring more uniform regulations across different territories. Such a system would streamline legal processes and foster a sense of international cooperation and shared responsibility in governing the Metaverse, promoting a more consistent and effective approach to online safety and regulation.

### *8.4. Lifting the Anonymity Veil*

The challenge of anonymity in the Metaverse, especially when addressing harmful behaviours like sexual harassment or fraud, necessitates a nuanced approach to revealing the true identities behind virtual avatars. A proposed solution involves registering avatars using real-world identifiers, such as government-issued IDs or social security numbers. This method could limit the number of avatars an individual can maintain and provide clarity on their age, gender, and nationality. However, this approach raises significant data protection concerns and requires a robust framework to safeguard sensitive user information.

Despite the anonymity users enjoy in the Metaverse, platforms typically can identify the individuals behind avatars through collected registration data, including IP addresses. In cases of severe misconduct, platforms are proposed to disclose the identity of the offending user. Such disclosures should be limited to serious cases to maintain system integrity and user trust, balancing the need for accountability with the right to privacy. Further, introducing statutory remedies specific to the Metaverse could hold individuals legally accountable for the actions of their avatars. This would circumvent the need for traditional legal standards used to pierce the corporate veil. In legal disputes involving Metaverse avatars causing real-world harm, pre-action discovery could compel the disclosure of the real person's identity behind the avatar. If the identity remains concealed, appointing a litigation representative to act on behalf of the avatar in real-world legal proceedings is a potential solution.

These strategies for lifting the veil of anonymity in the Metaverse are integral to the broader discussion of creating a safe and responsible virtual environment. They directly address earlier discussions about the complexities of consent and jurisdiction in the Metaverse, offering practical methods to hold users accountable for their actions in virtual spaces. Implementing these measures requires careful consideration of privacy

rights, data protection, and the potential impact on user experience. Striking a balance between the benefits of virtual anonymity and the responsibilities of identifiable presence is key to navigating the evolving legal and technological landscapes of the Metaverse (Cheong 2022).

#### *8.5. Role of Metaverse Platforms*

In the Metaverse, the responsibilities and liabilities of the platforms hosting these virtual spaces are critical areas for exploration. This need for clarity in platform responsibilities becomes particularly pertinent in light of regulatory movements like the European Union's upcoming Digital Services Act (DSA), which aims to define the liability of service providers, especially concerning the content on their platforms. Focusing on the role of Metaverse platforms, their potential liability hinges on fulfilling key responsibilities. In the specific context of addressing sexual harassment within the Metaverse, these responsibilities are twofold. Firstly, there is the regulation of content. Platforms are tasked with moderating and controlling the content circulating within their virtual environments. This duty involves not only detecting and removing harmful content, such as that constituting sexual harassment, but also balancing this with the users' rights to freedom of expression. The challenge lies in devising moderation systems that are effective yet sensitive to the nuances of user interaction in these virtual spaces. Secondly, user authentication plays a crucial role. Ensuring users' real-world identities is a potent strategy to discourage misconduct by tying virtual actions to real-world accountability. However, implementing user authentication processes brings forth privacy and data protection concerns, necessitating a nuanced approach that respects users' privacy while enhancing overall safety. Liabilities for Metaverse platforms arise primarily when these responsibilities are deviated from or neglected. Suppose a platform fails to regulate its content or verify user identities adequately, and this negligence results in instances of sexual harassment or abuse. In that case, the platform may face legal and regulatory repercussions. This scenario underscores the importance of proactive and robust management by platform providers to safeguard users and ensure a respectful and secure virtual environment. As the Metaverse continues to expand and integrate into various aspects of daily life, the imperative for these platforms to shoulder their share of responsibility in creating and maintaining safe virtual spaces becomes increasingly significant. The approach being adopted in the EU, as exemplified by the DSA, could provide a template for other jurisdictions, highlighting the need for clear, enforceable regulations and defined responsibilities for digital service providers in this evolving digital era.

Platforms operating within the Metaverse have the opportunity to harness artificial intelligence (AI) in their efforts to regulate content and user behaviour effectively. With its advanced capabilities, AI can be a powerful tool in pre-empting and mitigating various cyber threats and cybercrimes. Its potential in this realm is already being demonstrated by social media platforms like Facebook, which employ AI technologies to detect and manage misinformation and harmful content. The application of AI in the Metaverse can extend to several key areas. Firstly, AI can be instrumental in content moderation, using sophisticated algorithms to identify and filter out content that violates platform policies or poses potential harm. This includes detecting instances of sexual harassment, hate speech, and other forms of abusive behaviour. AI systems can be trained to recognise patterns and indicators of such content, enabling quicker and more efficient responses compared with manual moderation. Furthermore, AI can play a crucial role in enhancing user authentication processes. By analysing user behaviour and interaction patterns, AI can help identify suspicious or anomalous activities that may indicate fraudulent or malicious accounts. This capability can be advantageous in a virtual environment like the Metaverse, where the anonymity of users can pose significant challenges to platform governance.

However, using AI in these contexts must be approached with caution. While AI offers remarkable efficiency and scalability, it is not infallible. Issues such as bias in algorithmic decision-making and the potential for false positives or negatives in content moderation

necessitate a balanced approach. It is crucial for platforms to complement AI moderation with human oversight, ensuring that decisions, especially those with significant impacts on user experience and rights, are fair and just. Additionally, the ethical implications of using AI for surveillance and data analysis in the Metaverse must be considered. Protecting user privacy and ensuring transparency in how AI systems are used for content regulation and behaviour monitoring is paramount. Platforms must establish clear guidelines and ethical standards for AI usage, maintaining an open dialogue with users about how their data are used and AI-driven decisions are made. Video game developers have started using AI to detect practices such as cheating (Jonnalagadda et al. 2021; Mintlounge n.d.). Metaverse platforms may also use AI to detect identity theft, offensive speech, and instances of bodily violation of avatars (Lin and Latoschik 2022). Platforms can also be made responsible for adopting user authentication mechanisms. These can be biometrics-based, such as camera photo ID verifications, voice recognition, and fingerprints (Semple et al. 2010). Authentication of physiological biometrics, such as iris scans, ECG, and EEG, can be performed using VR devices (Ryu et al. 2021). User authentication will be an important step in ensuring that platforms can control the activities of users and carry out their responsibilities effectively.

## 9. Conclusions

This exploration of the Metaverse, a groundbreaking domain for social interaction, concludes with the observation that our current legal frameworks are woefully unprepared to address the unique challenges it presents, especially in terms of sexual violence. This article serves as a crucial step towards understanding and developing a comprehensive legal framework tailored for the Metaverse, focusing on ensuring the safety and dignity of all its participants. The Metaverse, with its immersive and interactive nature, blurs the lines between virtual and physical realities, creating new complexities in defining and regulating behaviour. Our discussion underscores the necessity for novel legal definitions of virtual harm, expanding beyond the confines of physical-world harms to include the multifaceted consequences of actions in virtual spaces. This broadened perspective is vital in acknowledging the psychological and emotional impacts of virtual interactions.

The role of consent mechanisms in the Metaverse has been highlighted as a paramount concern. Clear protocols for obtaining affirmative consent in virtual interactions are necessary to protect users from unwanted experiences. This involves educating users on norms and etiquette within the Metaverse and equipping them with tools to control their interactions, like the “Personal Boundary” feature introduced by Meta. The global nature of the Metaverse poses significant jurisdictional challenges, necessitating international cooperation and the establishment of a common legal framework. This framework should address key issues such as consent, anonymity, and financial transactions, ensuring consistent border regulation. Lifting the anonymity veil in the Metaverse is another critical aspect that requires attention. Implementing mechanisms for user authentication through real-world identifiers could mitigate accountability issues, but this raises concerns about data protection and user privacy. Therefore, platforms need to balance user verification with the ethical handling of sensitive information.

Furthermore, this article emphasises the evolving role of Metaverse platforms. These platforms can no longer be regarded as mere intermediaries; they must actively participate in content regulation and user safety. This shift in responsibility suggests that platforms will need to develop robust moderation systems and contribute to creating a safe virtual environment. We argue that the journey towards regulating the Metaverse is multi-dimensional, requiring concerted efforts from lawmakers, technologists, and users. The legal framework for the Metaverse needs to be dynamic, adapting to its evolving nature while upholding the principles of safety, respect, and accountability. This study provides an analytical and comprehensive foundation for these efforts, offering insights and recommendations that can guide future legal and regulatory approaches in this novel digital frontier.

**Author Contributions:** Conceptualization, S.B., M.C., and K.-S.C.; methodology, S.B., M.C., and K.-S.C.; formal analysis, S.B., M.C., and K.-S.C.; investigation, S.B., M.C., and K.-S.C.; resources, S.B., M.C., and K.-S.C.; data curation, S.B., M.C., and K.-S.C.; writing—S.B., M.C., and K.-S.C.; writing—S.B., M.C., and K.-S.C.; project, S.B., M.C., and K.-S.C.; funding acquisition, S.B., M.C., and K.-S.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by Naif Arab University for Security Sciences under Grant No. NAUSS-23-R03.

**Data Availability Statement:** The data supporting the findings of this study are available from the authors upon reasonable request.

**Acknowledgments:** The authors are grateful to the Vice-Presidency for Scientific Research at Naif Arab University for Security Sciences for encouraging this work. Additionally, they thank Kunika Agarwal from NUJS for her valuable research assistance.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

- Abbas, Lina, and Hamzeh Dodeen. 2022. Body Dysmorphic Features among Snapchat users of “Beauty-Retouching of Selfies” and its Relationship with Quality of Life. *Media Asia* 49: 196–212. [CrossRef]
- Allam, Zaheer, Ayyoob Sharifi, Simon E. Bibri, David S. Jones, and John Krogstie. 2022. The Metaverse as a Virtual Form of Smart Cities: Opportunities and Challenges for Environmental, Economic, and Social Sustainability in Urban Futures. *Smart Cities* 5: 771–801. [CrossRef]
- Belamire, Jordan. 2016. My First Virtual Reality Groping. *Medium*. October 21. Available online: <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee> (accessed on 16 February 2024).
- Benrimoh, David, Forum D. Chheda, and Howard C. Margolese. 2022. The Best Predictor of the Future—the Metaverse, Mental Health, and Lessons Learned From Current Technologies. *JMIR Mental Health* 9: e40410. [CrossRef]
- Bhat, P. Ishwara, ed. 2020a. Comparative Method of Legal Research: Nature, Process, and Potentiality. In *Idea and Methods of Legal Research*. Oxford: Oxford University Press, pp. 267–99.
- Bhat, P. Ishwara, ed. 2020b. Doctrinal Legal Research as a Means of Synthesizing Facts, Thoughts, and Legal Principles. In *Idea and Methods of Legal Research*. Oxford: Oxford University Press, pp. 143–68.
- Bill Information. 2022. 성폭력범죄의 처벌 등에 관한 특례법 일부개정법률안(민형배의원 등 13 인). Available online: [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_R2P2V0H4N0C1N1M1J2U4A2T7V2D5x9](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_R2P2V0H4N0C1N1M1J2U4A2T7V2D5x9) (accessed on 16 February 2024).
- Blackwell, Lindsay, Nicole Ellison, Natasha Elliott-Deflo, and Raz Schwartz. 2019. Harassment in Social Virtual Reality: Challenges for Platform Governance. *Proceedings of the ACM on Human-Computer Interaction* 3: 1–25. [CrossRef]
- Cheong, Ben C. 2022. Avatars in the Metaverse: Potential Legal Issues and Remedies. *International Cybersecurity Law Review* 3: 467–94. [CrossRef]
- Cripps, Jenna, and Lana Stermac. 2018. Cyber-Sexual Violence and Negative Emotional States among Women in a Canadian University. *International Journal of Cyber Criminology* 12: 171–86.
- Cummings, James J., and Jeremy N. Bailenson. 2016. How Immersive Is Enough? A Meta-Analysis of the Effect of Immersive Technology on User Presence. *Media Psychology* 19: 272–309. [CrossRef]
- Dolan, Lisa. 2022. The Legal Ramifications of Virtual Harms: A Study into the Human Rights Implications of a Meta-Led Metaverse. Available online: <https://repository.gchumanrights.org/server/api/core/bitstreams/c391e556-0288-4e64-ba7c-01fd0beb57b1/content> (accessed on 16 February 2024).
- EPRS. 2022. Metaverse Opportunities, Risks and Policy Implications. Available online: [https://www.europarl.europa.eu/cmsdata/268589/eprs-briefing-metaverse\\_EN.pdf](https://www.europarl.europa.eu/cmsdata/268589/eprs-briefing-metaverse_EN.pdf) (accessed on 16 February 2024).
- European Council. 2022. Digital Services Act: Council and European Parliament Provisional Agreement for Making the Internet a Safer Space for European Citizens. Available online: <https://www.consilium.europa.eu/en/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/> (accessed on 16 February 2024).
- Fajar, Muhamad, David David, Pardomuan R. Sihombing, Hirau A. Kekal, Irfan Aditya, Reza Ilham, and Yoga S. Keswara. 2022. The Metaverse to Enhance Safety Campaign toward Shipping Industry (Case Study: The Development and Implementation of Metaverse in Government-Owned Corporation). *International Journal of Emerging Technology and Advanced Engineering* 12: 1–11. [CrossRef]
- Forkast. 2022a. Sexual Harassment in Metaverse Triggers S. Korean Government Response. Available online: <https://forkast.news/headlines/sexual-harassment-metaverse-government/> (accessed on 16 February 2024).
- Forkast. 2022b. South Korea Struggles to Prevent Sexual Harassment of Minors in the Metaverse. Available online: <https://forkast.news/south-korea-sexual-harassment-minors-metaverse/> (accessed on 16 February 2024).
- Freeman, Guo, Samaneh Zamanifard, Divine Maloney, and Dane Acena. 2022. Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction* 6: 1–30. [CrossRef]

- Gomez, Juliana, Shane Johnson, Herve Borrión, and Samantha Lundrigan. 2024. A Scoping Study of Crime Facilitated by the Metaverse. *Futures* 157: 103338. [CrossRef]
- Gonzalez-Franco, Mar, Anthony Steed, Steve Hoogendyk, and Eyal Ofek. 2020. Using Facial Animation to Increase the Enfacement Illusion and Avatar Self-Identification. *IEEE Transactions on Visualization and Computer Graphics* 26: 2023–29. [CrossRef]
- Gu, Jinlei, Jiacun Wang, Xiwang Guo, Guanjun Liu, Shujin Qin, and Zhiliang Bi. 2023. A Metaverse-Based Teaching Building Evacuation Training System With Deep Reinforcement Learning. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 53: 2209–19. [CrossRef]
- Jesse, Lake. 2019–2020. Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection. *Emory Law Journal* 69: 833.
- Jonnalagadda, Aditya, Iuri Frosio, Seth Schneider, Morgan McGuire, and Joohwan Kim. 2021. Robust Vision-Based Cheat Detection in Competitive Gaming. *Proceedings of the ACM on Computer Graphics and Interactive Techniques* 4: 1–18. [CrossRef]
- Kalaf, Juliana, Evandro S. F. Coutinho, Liliane M. P. Vilete, Mariana P. Luz, William Berger, Mauro Mendlowicz, Eliane Volchan, Sergio B. Andreoli, Maria I. Quintana, Jair De Jesus Mari, and et al. 2017. Sexual Trauma is more Strongly Associated with Tonic Immobility than other Types of Trauma—A Population based Study. *Journal of Affective Disorders* 215: 71–76. [CrossRef]
- Kalyvaki, Maria. 2023. Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction. *Journal of Metaverse* 3: 87–92. [CrossRef]
- Kasiyanto, Safari, and Mustafa R. Kilinc. 2022. The Legal Conundrums of the Metaverse. *Journal of Central Banking Law and Institutions* 1: 299–322. [CrossRef]
- Keenan, Marie, and Estelle Zinsstag. 2022. Sexual Violence, Criminal Legal Frameworks, and the Need for Reform. In *Sexual Violence and Restorative Justice*. Edited by Marie Keenan and Estelle Zinsstag. Oxford: Oxford University Press, pp. 53–85.
- Kierkegaard, Sylvia. 2008. Cybering, Online Grooming and Ageplay. *Computer Law & Security Review* 24: 41–55. [CrossRef]
- Kim, So J., and Sunha Bae. 2021. Korean Policies of Cybersecurity and Data Resilience. Available online: <https://carnegiendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164> (accessed on 16 February 2024).
- Kim, Soyeon, and Eunjoon Kim. 2023. Emergence of the Metaverse and Psychiatric Concerns in Children and Adolescents. *Soa Chongsomyon Chongsin Uihak* 34: 215–21. [CrossRef]
- King, Daniel L., Samuel R. Chamberlain, Natacha Carragher, Joel Billieux, Dan Stein, Kai Mueller, Marc N. Potenza, Hans J. Rumpf, John Saunders, Vladan Starcevic, and et al. 2020. Screening and Assessment Tools for Gaming Disorder: A Comprehensive Systematic Review. *Clinical Psychology Review* 77: 101831. [CrossRef]
- Laue, Christian. 2011. Crime Potential of Metaverses. In *Virtual Worlds and Criminality*. Edited by Kai Cornelius and Dieter Hermann. Berlin and Heidelberg: Springer, pp. 19–29.
- Lee, Dong I. 2022. A Study on the Countermeasures of Avatar Sex Crime. *Forum of Public Safety and Culture* 19: 155–70. [CrossRef]
- Lee, Hyun W., Sanghoon Kim, and Jun P. Uhm. 2021. Social Virtual Reality (VR) Involvement Affects Depression When Social Connectedness and Self-Esteem Are Low: A Moderated Mediation on Well-Being. *Frontiers in Psychology* 12: 753019. [CrossRef]
- Lee, Jin H. 2022. A Legal Brief Study of Metaverse. *Liberal Arts Innovation Center* 9: 63–88. [CrossRef]
- Lee, Junyoung, and Heungki Min. 2022. Review of Legal Protection Measures against Security Threats Related to Metaverse. *Korean Association of Public Safety and Criminal Justice* 31: 321–44. [CrossRef]
- Lee, Won S. 2022. A Study on the Role of criminal law in Metaverse. *Institute for Legal Studies Chonnam National University* 42: 177–202. [CrossRef]
- Lemley, Mark A., and Eugene Volokh. 2018. Law, Virtual Reality, and Augmented Reality. *University of Pennsylvania Law Review* 166: 1051–66. [CrossRef]
- Lin, Jinghuai, and Marc E. Latoschik. 2022. Digital Body, Identity and Privacy in Social Virtual Reality: A Systematic Review. *Frontiers in Virtual Reality* 3: 974652. [CrossRef]
- Lorenzo-Dus, Nuria, and Cristina Izura. 2017. “Cause ur Special”: Understanding Trust and Complimenting Behaviour in Online Grooming Discourse. *Journal of Pragmatics* 112: 68–82. [CrossRef]
- Marshall, Angus M., and Brian C. Tompsett. 2023. The Metaverse—Not a New Frontier for Crime. *WIREs Forensic Science* 6: e1505. [CrossRef]
- Mintlounge. n.d. A New AI Innovation Aims to Stop Cheating in Multiplayer Video Games. Available online: <https://lifestyle.livemint.com//smart-living/innovation/a-new-ai-innovation-aims-to-stop-cheating-in-multiplayer-video-games> (accessed on 16 February 2024).
- Montefiore, Thomas, and Paul Formosa. 2022. Resisting the Gamer’s Dilemma. *Ethics and Information Technology* 24: 31. [CrossRef]
- Newton, Casey. 2021. Mark in the Metaverse. *The Verge*. June 22. Available online: <https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview> (accessed on 16 February 2024).
- Qin, Hua X., Yuyang Wang, and Pan Hui. 2022. Identity, Crimes, and Law Enforcement in the Metaverse. *arXiv* arXiv:2210.06134.
- Ramirez, Erick J. 2022. *The Ethics of Virtual and Augmented Reality: Building Worlds*. New York: Routledge.
- Ramirez, Erick J., Shelby Jennett, Jocelyn Tan, Sydney Campbell, and Raghav Gupta. 2023. XR Embodiment and the Changing Nature of Sexual Harassment. *Societies* 13: 36. [CrossRef]
- Reeves, Carla. 2013. Fantasy Depictions of Child Sexual Abuse: The Problem of Ageplay in Second Life. *Journal of Sexual Aggression* 19: 236–46. [CrossRef]
- Reitz, John C. 1998. How to Do Comparative Law. *The American Journal of Comparative Law* 46: 617–36. [CrossRef]

- Robinson, Laura, Jeremy Schulz, Grant Blank, Massimo Ragnedda, Hiroshi Ono, Bernie Hogan, Gustavo S. Mesch, Shelia R. Cotten, Susan B. Kretchmer, Timothy M. Hale, and et al. 2020. Digital Inequalities 2.0: Legacy Inequalities in the Information Age. *First Monday* 25: 1–27. [CrossRef]
- Ryu, Riseul, Soonja Yeom, Soo K. Kim, and David Herbert. 2021. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. *IEEE Access* 9: 34541–57. [CrossRef]
- Semple, Mid, Jeffrey Hatala, Patricia Franks, and Margherita A. Rossi. 2010. Is Your Avatar Ethical? on-Line Course Tools That are Methods for Student Identity and Verification. *Journal of Educational Technology Systems* 39: 181–91. [CrossRef]
- Sharma, Vivek. 2022. Introducing a Personal Boundary for Horizon Worlds and Venues. Available online: [https://www.meta.com/blog/quest/introducing-a-personal-boundary-for-horizon-worlds-and-venues/?utm\\_source=rakuten&utm\\_medium=affiliate&utm\\_campaign=nOD\\_rLJHOac-1bAgFIPDF2\\_nBHDeeKzrKQ&MID=43993&LSNSUBSITE=Omitted\\_nOD\\_rLJHOac&utm\\_term=exclusive&utm\\_content=ad](https://www.meta.com/blog/quest/introducing-a-personal-boundary-for-horizon-worlds-and-venues/?utm_source=rakuten&utm_medium=affiliate&utm_campaign=nOD_rLJHOac-1bAgFIPDF2_nBHDeeKzrKQ&MID=43993&LSNSUBSITE=Omitted_nOD_rLJHOac&utm_term=exclusive&utm_content=ad) (accessed on 16 February 2024).
- Sum of US. 2021. Metaverse: Another Cesspool of Toxic Content. Available online: [https://www.eko.org/images/Metaverse\\_report\\_May\\_2022.pdf](https://www.eko.org/images/Metaverse_report_May_2022.pdf) (accessed on 16 February 2024).
- Volante, Matias, Sabarish V. Babu, Himanshu Chaturvedi, Nathan Newsome, Elham Ebrahimi, Tania Roy, Shaundra B. Daily, and Tracy Fasolino. 2016. Effects of Virtual Human Appearance Fidelity on Emotion Contagion in Affective Inter-Personal Simulations. *IEEE Transactions on Visualization and Computer Graphics* 22: 1326–35. [CrossRef]
- Vranken, Jan B. 2011. Methodology of Legal Doctrinal Research: A Comment on Westerman. In *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline*. Oxford: Hart, pp. 111–21.
- Wiederhold, Brenda K. 2022. Sexual Harassment in the Metaverse. *Cyberpsychology, Behavior, and Social Networking* 25: 479–80. [CrossRef]
- Wodajo, Kebene. 2022. Mapping Invisibility and Structural Injustice in the Digital Space. *Journal of Responsible Technology* 9: 100024. [CrossRef]
- Wu, Jiajing, Kaixin Lin, Dan Lin, Ziyue Zheng, Huawei Huang, and Zibin Zheng. 2023. Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. *IEEE Open Journal of the Computer Society* 4: 37–49. [CrossRef]
- Yang, Lijuan. 2023. Recommendations for Metaverse Governance based on Technical Standards. *Humanities and Social Sciences Communications* 10: 253. [CrossRef]
- Ye, Deng, and Xinjuan Chang. 2022. An Analysis of the Legal Nature of Sexual Insults in the Meta-Universe. *Gachon Law Review* 15: 3–24. [CrossRef]
- Zhao, Ruoyu, Yushu Zhang, Youwen Zhu, Rushi Lan, and Zhongyun Hua. 2023. Metaverse: Security and Privacy Concerns. *Journal of Metaverse* 3: 93–99. [CrossRef]
- Zytco, Douglas, and Jonathan Chan. 2023. The Dating Metaverse: Why We Need to Design for Consent in Social VR. *IEEE Transactions on Visualization and Computer Graphics* 29: 2489–98. [CrossRef]

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.