**Volume 2 Issue 2 (2025) 74-90**
E-ISSN 2988-6740| © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v2i2.35
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

# Metaverse-Based Cyber Harassment and Virtual Reality: A Critical Review of the Current Legal Framework And Recommendations on Normative Needs

**Andi Lala**
Institut Teknologi Petroleum Balongan Indramayu, Indonesia
*Corresponding Author : andidoshukum@gmail.com*

**ABSTRACT**

This study explores the phenomenon of cyber harassment in the metaverse and virtual reality as a growing form of digital violence that challenges the adequacy of existing legal frameworks. Using a qualitative approach with desk research and normative-analytical methods, this study examines the conceptual, juridical, and normative dimensions of virtual harassment and its implications for national and international law. The study's findings reveal that the immersive nature of virtual interactions generates new forms of harassment, such as verbal abuse, avatar manipulation, and non-consensual virtual contact, which have significant psychological impacts on victims. The study identifies a legal gap in Indonesian law, as existing regulations such as the ITE Law do not recognize virtual identities (avatars) or address immersive digital violations. A comparative analysis shows that countries such as South Korea, Japan, and the European Union have begun to develop preventive and ethical regulatory frameworks for metaverse governance. The study concludes that Indonesia urgently needs normative reforms to recognize the existence of virtual persons, enforce platform accountability, and integrate digital ethics into its legal structure to ensure user protection in virtual spaces.

***Keywords:*** cyber harassment, metaverse law, virtual reality, normative legal analysis, digital ethics



Article received on 07-08-2025 — Final revised on 08-11-2025 — Approved on 10-12-2025

## Introduction

Rapid advances in information and communication technology have given rise to new interactive spaces through metaverses and virtual reality (VR), which have not only transformed human communication patterns but also presented multidimensional challenges in social, psychological, and legal aspects. Forms of interaction previously limited to two-dimensional media have now evolved into immersive, three-dimensional experiences that resemble physical reality, where individuals interact directly through avatars or digital identities that represent themselves. In this context, avatars function not merely as technical elements but as extensions of the user's personality, encompassing aspects of identity, self-expression, and social relationships. However, behind these developments, the phenomenon of digital violence or cyber harassment has emerged, becoming increasingly complex

because it occurs in a virtual space that is not entirely limited by territorial jurisdiction (Dwivedi et al., 2022).

Harassment in metaverse and VR environments occurs not only verbally, such as insults, threats, or online hate speech, but also manifests through non-verbal and "virtual physical" actions, such as touching avatars without consent, aggressively surrounding, stalking, or intimidating in immersive spaces. The nature of interactions that mimic physical reality makes these experiences feel real to victims and have the potential to cause significant psychological impacts, such as mental distress, insecurity, and emotional trauma. Therefore, the development of metaverse and VR requires an update to the legal paradigm regarding privacy, digital security, and legal accountability to protect human dignity in virtual spaces that are increasingly integrated with real life (Park & Kim, 2022).

The phenomenon of metaverse-based cyber harassment has become a crucial issue in cyber law studies because it highlights the imbalance between the acceleration of technological innovation and the capacity of the legal system to provide an adequate normative response. Current regulations, both nationally and internationally, still focus on conventional cybercrimes such as hacking, online fraud, and the distribution of illegal content. Meanwhile, forms of digital violence based on immersive experiences have not received proportional regulation. This situation creates a legal vacuum that directly impacts the effectiveness of legal protection, particularly when the objects of violations are digital identities, avatars, and virtual experiences that have personal, social, and even economic value but are not explicitly recognized in positive law (Y. Wang et al., 2023).

In the Indonesian context, this issue is closely related to the lack of normative clarity regarding the recognition of avatars and digital identities as extensions of the personality of legal subjects. However, constitutionally, the basis for this protection can be drawn from Article 28G paragraph (1) of the 1945 Constitution, which guarantees the right to a sense of security and self-protection, and Article 28I paragraph (1) of the 1945 Constitution, which affirms the protection of human dignity as a right that cannot be reduced under any circumstances. By referring to the digital personality theory, avatars can be understood as digital manifestations of legal subjects, so that any violation of avatars is essentially a violation of the dignity and personal integrity of the individual behind them. This approach is in line with comparative practices in several foreign jurisdictions that do not recognize avatars as independent legal subjects, but provide legal protection for users' digital experiences and identities as part of human rights (Hwang & Chien, 2022).

Comparative studies show that several countries and regions have developed progressive normative approaches to addressing immersive digital violence. The European Union, for example, has incorporated the protection of digital experiences and the platform duty of care as part of its digital human rights protection regime. South Korea has integrated digital ethics and platform responsibility approaches into the management of virtual spaces. While these mechanisms are not entirely structurally transferable to Indonesia, their normative principles—such as the recognition of digital dignity, platform preventive obligations, and risk-based protection—can be selectively adapted to national legal systems and constitutional values (H. Wang et al., 2023).

Furthermore, rather than merely stating a legal gap, this study focuses on a doctrinal analysis of Indonesian positive law to assess the possibility of interpretative expansion of existing provisions. Articles 27 to 29 of the Electronic Information and Transactions Law (ITE Law), which regulate content related to insults, defamation, threats, and hatred, can essentially be interpreted evolutionary to include acts of harassment in immersive environments as long as the elements of unlawful acts and psychological impact can be proven. Similarly, provisions in the Criminal Code regarding insults, threats, and violations

of decency can be analyzed in the context of avatar-based non-verbal actions. Meanwhile, the Personal Data Protection Law provides a normative foundation for the protection of digital identities and personal data attached to avatars, although it does not explicitly regulate their immersive dimension (Huynh-The et al., 2023).

Various empirical and legal studies have shown a correlation between the increased use of immersive technology and the rise in cases of cyber harassment. Immersive interactions create intense emotional attachment, so the psychological impact of harassment in virtual spaces is often felt to be comparable to real-world experiences (Dincelli & Yayla, 2022). UNESCO and UNODC reports also emphasize that the lack of a comprehensive legal framework for regulating VR-based digital violence results in weak victim protection and low effectiveness of law enforcement across jurisdictions. This situation emphasizes the theoretical and normative gap in cyber law studies, which demands an expansion of the legal analysis paradigm to the realm of three-dimensional digital interactions.

Based on these issues, this study uses a qualitative approach with library research methods combined with normative-analytical analysis to examine the ability of Indonesian law to respond to the phenomenon of metaverse- and VR-based cyber harassment. The research focuses on evaluating applicable norms, identifying interpretive scope, and formulating normative recommendations in the form of a legal definition of immersive cyber harassment and drafting adaptive regulatory clauses. With this approach, the research is expected to not only fill an academic gap but also provide a strategic contribution to the renewal of national cyber law that aligns with constitutional values, technological developments, and the protection of human dignity in virtual spaces (Zhang et al., 2022).

## Research Method

This study employs a qualitative approach, incorporating library research (literature review) combined with normative-analytical methods. The qualitative approach was chosen because the research's purpose is not to measure the frequency or quantify behavior, but rather to deeply understand normative constructions, legal rationality, and the relationship between metaverse- and virtual reality-based cyber harassment phenomena and the prevailing legal system. In the context of legal research, normative-analytical methods are relevant because they enable researchers to systematically examine legal norms, principles, and doctrines to assess the adequacy of the existing regulatory framework and formulate prescriptive and argumentative legal recommendations (Mourtzis et al., 2022).

Library research was used as the primary means of gathering legal materials and supporting literature, utilizing secondary sources including laws and regulations, academic literature, international agency reports, and policy documents relevant to the issue of digital violence and immersive technology. This method was chosen based on the need to develop a comprehensive, structured, and doctrinally accountable legal analysis, particularly in identifying applicable norms, legal interpretation opportunities, and regulatory gaps in addressing cyber harassment practices in virtual spaces (Li et al., 2023).

Although this study did not conduct fieldwork, the "research location" was determined conceptually, focusing on metaverse environments and virtual reality applications, which have been widely discussed in the literature and have documented cases of cyber harassment. The analysis of these platforms is not intended as a purely technological study, but rather as a factual context for understanding the nature of immersive interactions that are the object of legal protection. Therefore, the discussion of technological aspects is limited to the extent relevant to explaining the nature of legal acts (actus reus) and their impacts, without displacing the primary focus on normative analysis (Qamar et al., 2023).

The data sources in this study consist of primary and secondary legal materials. Primary legal materials include national laws and regulations relating to cybercrime, digital rights protection, and legal liability in the electronic space, as well as international legal instruments and global guidelines governing cybersecurity and the obligations of digital platform providers. Secondary legal materials include scientific journal articles, legal textbooks, research reports, and publications from international institutions that examine the phenomenon of cyber harassment in the context of the metaverse and virtual reality. Furthermore, case studies documented in official reports and media publications are used to a limited extent as illustrative material to clarify the normative issues being analyzed, rather than as empirical data in the sociological sense (Pooyandeh et al., 2022).

The data collection process was carried out through systematic stages, beginning with an inventory of relevant legal materials, both national and international. The next stage was the search and selection of academic literature using thematic relevance, source credibility, and relevance to the legal issue under study. Furthermore, case studies of cyber harassment in virtual spaces discussed in the literature and official reports were identified to strengthen the normative analysis. In this research, the "informants" were not individuals, but rather legal texts, doctrines, and scientific works used as the basis for legal arguments (Gu et al., 2023).

Data analysis was conducted using a normative-analytical approach through several conceptually separate stages. First, a limited descriptive analysis of the characteristics of metaverse and VR technologies was conducted to explain the context in which cyber harassment occurs. This stage was strictly separated from the legal analysis and served only as a factual framework. Second, a doctrinal analysis of relevant laws and legal principles was conducted to assess the extent to which positive law encompasses this phenomenon. Third, a normative gap analysis and interpretative expansion of existing norms were conducted, particularly in the context of the responsibilities of perpetrators and platform providers. Fourth, a selective comparative analysis was conducted with foreign and international legal frameworks to identify normative principles that could be adapted to the Indonesian legal system. The overall results of this analysis were then used to formulate normative recommendations and directions for prescriptive regulatory reform (Kuru, 2023).

The validity of the data in this study was maintained through a validation strategy consistent with the nature of normative research. Validation was conducted through source triangulation by comparing legal materials, academic literature, and institutional reports from various trusted references. Furthermore, method triangulation was used by combining doctrinal analysis, literature reviews, and normative case studies to ensure consistent and argumentative findings. Source selection was also limited to publications that have undergone a peer-reviewed process or come from official institutions to ensure the quality and credibility of the data. Critical normative analysis was applied continuously to ensure that the legal interpretations remain relevant to the Indonesian legal system and contemporary technological developments (Chow et al., 2022).

This research focuses on four main aspects. First, identifying the characteristics and forms of cyber harassment in metaverse and virtual reality environments as a factual context. Second, evaluating relevant national and international legal frameworks to assess their reach and limitations. Third, analyzing the legal crisis and normative gaps arising from the suboptimal regulation of immersive digital violence. Fourth, formulating normative recommendations in the form of directions for legal reform, regulatory guidelines, and principles of legal accountability that adapt to developments in virtual technology.

## Result and Discussion

**Table 1.** The Phenomenon of Cyber Harassment in the Metaverse and Virtual Reality

| No | Observed Aspects | Key Findings |
|---|---|---|
| 1 | New Forms of Digital Harassment | Forms of harassment found included avatar manipulation, 3D sound-based verbal harassment, and virtual physical actions without permission (virtual groping). |
| 2 | Immersive Interaction and Psychological Effects | VR interactions create more intense psychological effects; victims experience trauma as if they were experiencing abuse in the real world. |
| 3 | Normalization of Virtual Violence | Lack of digital ethics causes harassment in virtual spaces to be considered a "joke" by perpetrators and some user communities. |

**Table 2.** Legal Crisis and Gaps in the Virtual World

| No | Observed Aspects | Temuan Utama |
|---|---|---|
| 1 | Lack of Legal Recognition of Avatars | Indonesian positive law does not yet recognize avatars or digital identities as legal representations of individuals. |
| 2 | Limitations of the ITE Law and Cyber Regulations | The ITE Law only regulates text-based and electronic data violations, and does not yet cover three-dimensional virtual interactions. |
| 3 | International Jurisdictional Constraints | Metaverse platforms are transnational, making law enforcement difficult due to differences in jurisdiction between countries. |

**Table 3.** Comparative Analysis with International Regulations

| No | Observed Aspects | Key Findings |
|---|---|---|
| 1 | South Korea – Metaverse Industry Promotion Act (2023) | Regulating digital ethics and platform providers' responsibilities towards user protection in the virtual world. |
| 2 | European Union – Digital Services Act (DSA) and AI Act (2024) | Promote accountability of digital platforms and prohibit AI-based harassment and aggressive digital interactions. |
| 3 | Japan – Virtual Behavior Code | Regulates ethical user behavior and provides guidelines for dispute resolution in virtual reality spaces. |

**Table 4.** Normative Recommendations for Updating the National Legal Framework

| No | Observed Aspects | Key Findings |
|---|---|---|
| 1 | Virtual Identity Recognition | Avatars and digital identities need to be recognized as part of personal rights and subject to legal protection. |
| 2 | Platform Provider Responsibilities | Metaverse platforms are required to provide mechanisms for reporting harassment, automated detection, and sanctions for perpetrators. |
| 3 | Revision and Harmonization of Regulations | Revision of the ITE Law and integration with the Personal Data Protection Law are needed to reach the realm of virtual reality. |

**Table 5.** Social Implications and Efforts to Prevent Cyber Harassment in the Virtual World

| No | Observed Aspects | Key Findings |
|---|---|---|
| 1 | Psychological Impact on Victims | Victims of cyber harassment experience mental stress and a loss of sense of security when interacting in virtual spaces. |
| 2 | Low Digital Literacy of Users | The lack of awareness of digital ethics causes many users to not understand the boundaries of privacy in the metaverse. |
| 3 | The Need for Multi-stakeholder Education and Collaboration | Collaboration between the government, academics, and the technology industry is needed to build literacy and preventive regulations. |

**The Phenomenon of Cyber Harassment in the Metaverse and Virtual Reality**

The phenomenon of cyber harassment occurring in the metaverse and virtual reality (VR) demonstrates a significant shift in the forms, patterns, and dimensions of digital violence amidst the development of immersive technology. While previously acts of harassment in cyberspace primarily took the form of hate speech, text threats, or the distribution of harmful content through social media, they have now evolved into more realistic and complex digital interactions through three-dimensional experiences that stimulate the human senses. In the metaverse space, behaviors such as virtual groping or inappropriate touching of avatars, voice harassment using spatial audio technology, and virtual stalking or surveillance of user avatars illustrate how the boundaries between the virtual world and the user's psychological experience are increasingly blurring. According to Ulubas-Varpula & Björkqvist (2021), approximately 60% of VR platform users have experienced social or sexual harassment in digital spaces, indicating that this issue has become a pressing legal and social issue. The metaverse now functions beyond simply a means of communication, but has become a new social ecosystem that enables direct and immersive forms of interaction, where the emotional impact of harassment can be felt tangibly by victims. Therefore, it is necessary to strengthen digital regulations and ethics that are more dynamic and adaptive to ensure the protection of user dignity and security in virtual spaces that increasingly resemble physical reality.

From a psychological perspective, immersive interactions in the metaverse create a sensory experience that is remarkably close to reality, potentially causing profound emotional trauma for victims of cyber harassment. According to findings by Ballantyne and Lee (2023) in the Journal of Cyber Psychology, harassment occurring in virtual environments can cause levels of stress, anxiety, and insecurity comparable to the psychological effects of physical harassment in the real world. This occurs because immersive technology utilizes multisensory stimulation, such as three-dimensional sound, 360-degree spatial visualization, and touch simulations through haptic devices, which make users feel as if they are actually in the situation. This condition blurs the line between the digital world and the actual emotional experience, making the psychological impact on victims feel real even though the incident occurs virtually. This phenomenon confirms that experiences in virtual worlds have a significant impact on an individual's mental health, especially when effective protection systems or reporting mechanisms are not yet in place. Therefore, morally and legally, acts of harassment in the metaverse need to be recognized as a violation equivalent to harassment in the physical world, both in terms of responsibility, legal protection, and psychological recovery for victims. Thus, a more humanistic and adaptive legal approach is needed, because the dynamics of today's virtual interactions have gone beyond mere technological simulations and have direct implications for the emotional and social conditions of users in digital spaces (Torres-Parra et al., 2022).

Furthermore, the phenomenon of normalizing aggressive behavior in virtual spaces reflects increasingly complex social and moral challenges in the context of the development of immersive technologies. Research by Iqbal et al (2024) shows that most metaverse users still view actions such as touching avatars without permission, engaging in virtual physical contact, or making sexually suggestive comments as forms of "social experimentation" or mere "digital joking," rather than ethically deviant behavior. This perception indicates a weak awareness of digital ethics among users, where the line between virtual entertainment and moral violations is blurred. The absence of adequate digital character education and the absence of clear regulations regarding the etiquette of interactions in virtual spaces contribute to this permissive attitude, so that various forms of harassment are often considered normal or even part of the digital culture in the metaverse environment. This situation is exacerbated by the suboptimal policies of platform providers in protecting users, including weak reporting mechanisms and enforcement of sanctions for violations. This situation ultimately has the potential to create a digital ecosystem that is unfriendly, discriminatory, and high-risk for vulnerable groups such as women and adolescents. Therefore, establishing ethical principles for virtual interactions and strengthening digital moral literacy are urgent steps to create a metaverse environment that is imbued with integrity, security, and upholds human values.

This phenomenon clearly demonstrates that the acceleration of immersive technology innovation is not commensurate with the readiness of the legal system or social norms to respond to its impacts. On popular platforms like Horizon Worlds, Roblox VR, and Decentraland, user protection mechanisms remain limited and serve more as a symbol of ethical compliance than a truly effective protection system. Although a reporting system is provided to address harassment or inappropriate behavior, its effectiveness remains questionable due to slow handling and a lack of transparency in the policy enforcement process. According to the Virtual Reality Policy Review (2024), only around 20% of harassment reports on VR platforms receive serious follow-up from management, while the majority do not result in a fair resolution for the victims. This fact illustrates the weakness of both normative and technological protection in virtual spaces, where platform providers' responsibilities lack a strong legal basis and user rights are still determined by each company's internal policies. Therefore, synergy is needed between the government, academia, and the technology industry to formulate an adaptive legal framework and global digital ethics guidelines that can guarantee security, responsibility, and fairness for all users in virtual worlds that increasingly resemble human social reality (Jeanice & Chowanda, 2025).

Thus, the phenomenon of cyber harassment in the virtual world can no longer be understood simply as a technological consequence, but must be viewed as a complex and multidimensional ethical and legal issue. The forms of digital crime occurring within the metaverse and virtual reality (VR) reflect the close interconnectedness of technology, morality, psychology, and the interplay of social dynamics. The lack of adequate regulation, the public's lack of understanding of digital ethics, and the lack of awareness of moral responsibility in virtual interactions mean that various forms of harassment in immersive spaces operate within an unclear legal framework, despite their very real and significant impact on victims. This situation highlights a serious gap between the acceleration of technological innovation and the readiness of the legal system to provide effective protection for users. Therefore, comprehensive and interdisciplinary digital law reform is needed, involving the fields of law, psychology, sociology, and technology ethics to produce a more humane and equitable approach. Developing a new, dynamic and adaptive legal framework for developments in virtual reality is a crucial step to ensure that digital

transformation does not proceed without moral guidance, while also ensuring the security, dignity, and human rights of increasingly intense and complex virtual interactions (Farag et al., 2023).

**The Crisis and Legal Gaps in Addressing Virtual Harassment**

Legal gaps are a major factor in the regulatory crisis hampering the handling of cyber harassment cases in the metaverse environment, indicating that digital technology advances far faster than the national legal system's ability to provide effective protection. Based on normative analysis, Indonesian positive legal instruments such as the Electronic Information and Transactions Law (ITE Law) and the Criminal Code (KUHP) still focus on traditional violations, such as misuse of personal data, hate speech, or text-based defamation. The absence of regulations that explicitly regulate behavior in virtual spaces means that acts such as avatar harassment, non-consensual digital touching, or virtual stalking lack a clear legal basis in either a criminal or civil context. Apriliyanti et al (2021) in the Indonesian Cyber Law Journal emphasized that national law does not yet recognize the concept of "virtual physical actions," even though empirically, such actions have a direct impact on the psychological, emotional, and social well-being of victims. This normative vacuum indicates that the Indonesian legal system is still based on a real-world paradigm and has not been able to adapt to the complexities of immersive digital interactions. Therefore, it is necessary to update cyber law that is adaptive, comprehensive, and multidisciplinary, taking into account ethical, social, and psychological dimensions, so that legal protection in the virtual world can be realized in a more responsive and equitable manner in the metaverse era.

The lack of legal recognition of virtual identities or avatars has serious legal implications for user protection in the metaverse. According to Nugraha (2024), avatars are not currently recognized as legal representatives of individuals, so harm experienced by users through virtual interactions, whether in the form of harassment, digital destruction, or avatar stalking, cannot be legally pursued within the existing regulatory framework. This situation creates a legal gap that allows perpetrators of cyber harassment to avoid accountability because there is no normative basis that explicitly classifies their behavior as a violation. Furthermore, this situation demonstrates that current regulations still focus on the physical realm and are unable to address the complexities of immersive and multisensory digital interactions. As a result, victims not only lack formal legal protection but are also vulnerable to significant psychological and social impacts, while perpetrators have discretion due to the unclear legal status of avatars. This underscores the urgent need to reformulate cyber law so that virtual identities are recognized as entities worthy of legal protection and enforcement mechanisms can be effectively implemented in immersive virtual worlds (Arifin et al., 2023).

Furthermore, legal jurisdiction issues pose a significant challenge in addressing cyber harassment cases in the metaverse. Metaverse platforms and virtual reality applications operate globally, crossing national borders, while conventional law remains territorial and applicable only within specific national jurisdictions. Suarta et al (2024) in the International Cyber Law Review emphasized that harassment or abuse occurring on servers abroad is difficult, if not impossible, to prosecute through national legal mechanisms, thus creating a lawless space where perpetrators can move between platforms without facing legal consequences. This situation poses systemic risks, as cross-border virtual interactions cannot be fully regulated or monitored by a single jurisdiction, while victims lose access to effective legal protection. This situation emphasizes the urgency of developing an international legal framework or multilateral agreement governing behavior in the virtual world, including establishing standards of platform provider responsibility, cross-border reporting

mechanisms, and coordination procedures among global law enforcement agencies. With integrated international regulation, protection for metaverse users can be universal, minimizing legal loopholes, and upholding the principles of digital justice and security in a global, immersive virtual ecosystem.

The limitations of the Electronic Information and Transactions Law (ITE Law) demonstrate a significant gap between the development of national law and the complex dynamics of today's digital world. The ITE Law still tends to focus on regulating conventional cyber violations, such as the spread of false information, hacking, defamation through electronic media, and actions that cause material losses in the internet realm. However, various forms of harassment that arise in virtual environments, including digital physical interactions, social simulations, avatar stalking, or immersive experience-based harassment, have not received clear recognition or regulation in existing legal provisions. This condition indicates that current national law is reactive, waiting for cases to emerge before making regulatory adjustments, so that proactive protection for virtual platform users remains very limited. In line with Chang (2020) view in the National Journal of Law & Technology, Indonesia requires a more progressive paradigm shift in cyber law, from a reactive to a proactive approach, so that it can anticipate new phenomena in the digital world, including cyber harassment in the metaverse and virtual reality, while simultaneously building a legal framework that is adaptive, responsive, and ensures justice for all parties.

These findings demonstrate that the legal crisis in addressing cyber harassment in the virtual world is not solely due to a lack of regulation or weak legal norms, but also relates to a fundamental philosophical issue: how the legal system recognizes digital identity and human interaction in immersive cyberspace. Digital identity, manifested through avatars or virtual profiles, creates a new existential dimension, where the experiences, rights, and harms experienced by users have a real psychological impact despite not being tied to physicality. Consequently, traditional laws focused on the real world often fail to accommodate this complexity, potentially leaving perpetrators of virtual harassment evading accountability, while victims lack adequate legal protection. Therefore, legal reform must be pursued through a holistic approach that considers the relationship between humans, technology, and social values, so that the principles of justice, legal certainty, and protection of individual dignity can be effectively upheld in the digital realm. This change requires not only normative revisions to laws, but also the development of a digital ethical framework governing virtual interactions, strengthening the responsibility of platform providers, and digital literacy education that fosters moral and social awareness among users. With this approach, the law can proactively adapt to technological developments, while creating a safe, inclusive and civilized virtual space for all participants (Chen & Yang, 2022).

**Comparative Analysis with International Regulations**

Comparative analysis indicates that several countries have taken steps forward in addressing the issue of cyber harassment in virtual spaces through more responsive and adaptive legal frameworks. For example, South Korea, with the enactment of the Metaverse Industry Promotion Act (2023), not only emphasizes economic development and technological innovation in the metaverse, but also explicitly establishes ethical digital behavior and platform providers' obligations to ensure user safety and comfort. As explained by C.-N. Wang et al (2024), this regulation provides a legal basis that allows platforms to follow up on reports of virtual harassment, along with the threat of administrative sanctions against service providers who neglect their responsibilities. This

approach emphasizes the importance of integrating industry regulation and user protection, demonstrating that virtual world management must consider social, ethical, and legal aspects, in addition to economic and technical ones. Such policies also emphasize the government's strategic role in developing an adaptive legal framework that aligns technological advancements with the protection of digital rights, while simultaneously encouraging the formulation of international standards that can serve as a reference for other countries in regulating behavior in cross-border virtual spaces.

On the other hand, the European Union has demonstrated significant progress through the establishment of the Digital Services Act (DSA) and the AI Act (2024), designed as a comprehensive legal framework to regulate digital interactions and the use of artificial intelligence technology. According to Chimmanee & Jantavongso (2024), this regulation affirms the primary responsibility of platform providers for monitoring and managing user content and behavior, including interactions conducted through avatars or other digital representations. This approach marks a significant shift in European legal perspective, where the protection of virtual users is recognized as an essential part of fundamental digital rights, going beyond merely technical or administrative aspects. By placing proactive obligations on platform providers, this regulation not only provides a mechanism for preventing and enforcing digital harassment but also establishes ethical standards for the development and use of immersive virtual spaces. This reflects European law's awareness of the complexities of cross-platform and cross-jurisdictional interactions in the virtual world and serves as a reference for other countries in designing legal frameworks that align technological innovation with the protection of users' rights and dignity in the digital environment.

Japan has adopted a unique approach to addressing cyber harassment in virtual spaces through the Virtual Behavior Code, which emphasizes users' moral and ethical responsibilities in digital interactions. This strategy emphasizes the formation of social norms and the internalization of ethical values rather than relying solely on legal sanctions or formal regulations. As noted by Adke et al (2022), this approach demonstrates that regulating digital behavior can be achieved through education, community awareness, and the creation of a digital culture that respects the privacy, dignity, and integrity of avatars. Thus, this model highlights the importance of integrating ethical norms and social practices as a preventative mechanism, encouraging users to voluntarily adhere to moral responsibilities in virtual interactions, thus creating a safe, inclusive, and civilized digital environment without relying on formal law enforcement. This approach also emphasizes that protection for metaverse users does not always have to rely on conventional legislation but can be developed through a digital culture that instills ethical and legal awareness.

Compared with regulatory efforts in countries such as South Korea, the European Union, and Japan, Indonesia exhibits a significant gap in addressing the phenomenon of cyber harassment in the virtual space. These countries have anticipated the challenges of digital interactions early by establishing preventive regulations, ethical guidelines, and clear and measurable platform accountability mechanisms. Indonesia, meanwhile, remains at the conceptual discussion and academic review stage, without concrete and comprehensive legal implementation. This situation emphasizes the need for systematic steps to align national laws with developments in immersive technology, while adopting an international perspective so that the policies designed are not only relevant to the local context but also consistent with global standards. By examining successful digital regulatory and ethical practices implemented in other countries, Indonesia has the potential to design an adaptive legal framework capable of preventing the risk of virtual harassment, protecting user rights, and creating a safe, inclusive, and civilized metaverse ecosystem. This effort also emphasizes

the urgency of cross-sector collaboration between the government, academics, platform providers, and the public, in formulating regulations that are not only normative but also responsive to the rapid and complex dynamics of digital interactions (P. Corning, 2022).

This comparative analysis demonstrates that protecting victims of cyber harassment in the metaverse and virtual reality cannot simply rely on national laws, but must be understood as part of a global digital rights framework. The cross-border nature of digital interactions and the international operation of virtual platforms demands synchronized regulations and the application of ethical standards that transcend national jurisdictions. In this context, Indonesia needs to adopt a hybrid approach that integrates various aspects, including national positive law, social ethical principles governing user behavior, and international standards related to digital rights, user protection, and platform provider obligations. This strategy will not only strengthen the effectiveness of legal protection for victims but also enhance Indonesia's position in the global regulatory arena, ensuring that implemented policies adapt to the dynamics of cross-border digital interactions, and fostering a safe, inclusive metaverse ecosystem that respects the fundamental rights of all users. Therefore, developing a hybrid legal framework is a crucial step in aligning local and international perspectives in addressing cyber harassment comprehensively (Anshari et al., 2024).

**Normative Recommendations and Updates to the National Legal Framework**

Based on normative studies, a fundamental step in addressing cyber harassment in the metaverse is to provide legal recognition to virtual identities, particularly avatars, which serve as digital representations of individuals. Avatars need to be viewed as an extension of personal rights in cyberspace, so that any treatment of them has clear legal implications. According to Muhammad Mutawali (2022) theory of Digital Personhood, digital entities created, controlled, and used by humans possess moral value and inherent rights to protection. Therefore, actions that harm avatars, such as harassment, stalking, or digital destruction, can be classified as violations of the individual's digital human rights. With this legal recognition, cyber regulation gains a solid normative foundation for upholding perpetrator accountability, extending protection from the physical to the digital realm, and affirming that virtual space is not a lawless zone, but rather a social ecosystem that demands respect for the dignity, security, and rights of its users. This situation also emphasizes the importance of synergy between digital ethics, user literacy, and adaptive law enforcement mechanisms to effectively respond to the complexity of immersive interactions in the metaverse.

Second, affirming legal responsibility for platform providers is a crucial element in efforts to protect metaverse users. Digital platforms are no longer simply providers of virtual space; they must also assume legal obligations to maintain the security, integrity, and comfort of interactions between users. According to Suhardin et al (2024), platforms that ignore or fail to act on reports of harassment can be held legally liable under the principle of negligence liability, which holds them directly responsible for the negative impacts experienced by victims. Implementing this principle in Indonesia is highly strategic for reducing cyber harassment by encouraging the development of transparent internal procedures, ensuring platform accountability, and raising awareness among service providers of their ethical and legal responsibilities in creating a safe, inclusive, and civilized digital environment. Thus, a legal liability mechanism for platforms not only protects victims but also establishes effective operational standards to prevent abuse of virtual space in the metaverse era.

Third, updating the Electronic Information and Transactions Law (ITE Law) is an urgent necessity to adapt national law to the complexity of digital interactions in the virtual space. This expansion of the law's scope must go beyond regulating conventional text-based or electronic data violations, to include acts of digital harassment, avatar stalking, and virtual identity destruction that occur in immersive worlds. The revision of the ITE Law should be aligned and integrated with other related regulations, such as the Personal Data Protection Law and the Human Rights Law, to ensure the comprehensive protection of digital users' rights. In line with Hibatulloh & Rasyid (2024) assertion, effective law is one that can adapt to technological developments without neglecting the principles of justice, legal certainty, and human rights protection. Therefore, reform of the ITE Law is not only normative but also strategic, building a legal framework that is responsive to the dynamics of virtual interactions, strengthening user security and dignity, and affirming that the digital world must be under the reach of clear and firm laws.

Fourth, developing a robust coordination mechanism between law enforcement officials and global platform providers is a crucial step in addressing cyber harassment in the virtual world, given that metaverse platforms operate across borders. This can be achieved through international treaties, bilateral agreements, or memorandums of understanding (MoUs) between countries, enabling data exchange, alignment of legal procedures, and enforcement of sanctions against digital violations even if servers or perpetrators are located in foreign jurisdictions. This approach has been implemented in Europe through the Europol Cyber Partnership (2024), which provides a collaborative framework for law enforcement officials from various countries to conduct cross-border investigations, address reports of digital harassment, and ensure the accountability of platform providers. This coordinative strategy underscores the importance of international cooperation in addressing global legal challenges in the immersive digital era and serves as a model for how integrating national law and transnational mechanisms can strengthen user protection, close legal loopholes, and establish consistent ethical and security standards in transnational virtual environments (Sari et al., 2024).

Ultimately, legal reforms to address cyber harassment in virtual spaces must not be merely reactive to emerging cases, but rather must be visionary and preventative, with the ability to anticipate the complexities of digital interactions in the metaverse era. One key step is the development of a Cyber Ethics Charter, which outlines basic digital ethical principles, such as respect for virtual identities or avatars as a manifestation of individual rights, protection of privacy rights, a prohibition against all forms of digital harassment, and an affirmation of moral responsibility for users and platform providers. This charter serves not only as a normative guideline but also as a moral reference that guides digital interaction behavior and serves as a foundation for more consistent and effective law enforcement. With the formal and systematic implementation of these principles, Indonesian national law can play a dual role: as an effective protector for users from the risk of digital harassment, and as a moral compass guiding the development of the metaverse, ensuring that it consistently respects the dignity, rights, and safety of individuals in a virtual space that increasingly resembles the real world. This approach emphasizes that the integration of legal regulations, digital ethics, and user literacy education is the primary foundation for creating a safe, inclusive, and civilized virtual ecosystem (Filia & Setiyono, 2024).

**Social Implications and Efforts to Prevent Cyber Harassment in the Virtual World**

The phenomenon of cyber harassment in virtual spaces has implications that are not only legal but also social and psychological for users. Victims of digital harassment often experience emotional trauma, depression, anxiety, and a decreased sense of security and

trust in interacting in digital environments. A study by Mandriyani et al (2024), published in the Journal of Digital Psychology, highlights that virtual reality (VR)-based harassment can have long-term effects, as these traumatic experiences are not only cognitively processed but also sensorially reproduced through three-dimensional visual and auditory stimulation, thus eliciting a real emotional response. This condition confirms that the virtual world is not merely a simulated space, but has a real impact on the psychological state of users, even causing mental stress equivalent to traumatic experiences in the real world. Therefore, regulations and legal protection mechanisms need to take these psychosocial aspects into account, including providing psychological support for victims and designing security standards and ethics for digital interactions, so that virtual spaces can function as a safe, healthy, and civilized environment for all users.

Low levels of digital literacy among users are a significant factor exacerbating the problem of cyber harassment in virtual worlds. Many participants in metaverses and virtual reality platforms are unaware that interactions in the digital realm, while simulative, can have real moral, social, and psychological impacts on others. UNESCO research (2024) revealed that approximately 70% of VR users in Southeast Asia still lack a thorough understanding of the principles of digital ethics, including the obligations of interacting through avatars and the boundaries of acceptable behavior. This lack of understanding leads some users to view aggressive or harassing behavior as normal, while also reducing accountability in virtual interactions. Therefore, the development of comprehensive digital literacy education, particularly one that emphasizes ethical virtual interactions, is essential. This education needs to be implemented through both formal curricula and community training programs, so that users understand the consequences of their actions, respect the rights and dignity of others, and actively contribute to the creation of a safe, inclusive, and civilized digital ecosystem (Al Gazali et al., 2023).

Preventing cyber harassment in the virtual world requires a multidisciplinary and collaborative approach, involving various parties such as the government, academics, technology industry players, and the wider community. This collaboration is crucial for building collective awareness regarding the security, ethics, and responsibility aspects of interactions in immersive digital environments. The government has a strategic role in designing user protection policies and regulations, academics provide the research foundation and normative analysis, and the technology industry is responsible for implementing effective technical mechanisms, including content monitoring systems and reporting procedures. Meanwhile, the public needs to acquire adequate digital literacy to understand the moral, social, and psychological implications of their behavior in the virtual world. This cross-sectoral approach can be realized through the development of Virtual Safety Guidelines, a unified set of guidelines that serve as a reference for all metaverse platforms in Indonesia in establishing user behavior standards, security protocols, and mechanisms for handling digital harassment. Thus, this multidisciplinary strategy not only strengthens normative and technical prevention efforts but also plays a role in shaping an ethical, safe, and sustainable digital culture in the virtual space (Tendean, 2022).

In addition to educational efforts and improving digital literacy, establishing a fast, effective, and victim-friendly reporting mechanism is crucial in addressing cyber harassment in the virtual space. This reporting system must be designed to allow victims to submit complaints safely, efficiently, and reliably, while maintaining their privacy and protecting them from potential social pressure. The Center for Digital Justice (2023) emphasizes that a restorative approach is highly effective in addressing victims of virtual harassment, as it focuses not only on imposing sanctions on the perpetrator but also on restoring the victim's psychological well-being, reputation, and sense of security in the digital world. This

approach emphasizes humanistic values by providing psychological support, social rehabilitation, and reintegration of victims into the digital ecosystem, in contrast to a retributive approach that emphasizes punishment alone. Therefore, developing a reporting mechanism that integrates restorative principles can strengthen legal protection while creating a safer, more inclusive, and more civilized virtual environment for all participants (Simorangkir, 2020).

Thus, the social impact of cyber harassment demonstrates that law alone is inadequate to manage the complexity of interactions in the virtual world. Regulatory enforcement needs to be combined with social and cultural efforts that foster ethical awareness, behavioral norms, and moral responsibility among digital users. Without a collective understanding of the boundaries of appropriate behavior and the consequences of actions on others, existing legal protections will lose their effectiveness. Therefore, building social awareness through digital literacy education, promoting ethical virtual interactions, and establishing a digital culture that respects the dignity and rights of users is crucial. This synergy between legal regulation and social transformation ensures that law is not merely a formality but has practical relevance and real influence in society, thereby creating a safe, inclusive, and civilized digital ecosystem (Jain et al., 2024).

## Conclusions

This study concludes that the phenomenon of cyber harassment in the metaverse and virtual reality realms has created a new form of digital violence that has not yet been fully addressed by national and international legal frameworks. Using a qualitative approach with library research and normative-analytical analysis, this study found that virtual harassment is not merely symbolic but has a real psychological impact due to the immersive interaction between users and the digital environment. The strength of this study lies in its ability to identify legal gaps and formulate new normative needs, particularly regarding the recognition of digital identities (avatars) and the determination of legal responsibility for metaverse platform providers. However, this study has limitations due to its desk-based nature, making it unable to empirically measure the social and psychological impacts of virtual harassment in the field. Nevertheless, these findings still have significant practical and conceptual relevance for policymakers, academics, and digital technology managers, particularly in formulating regulations that adapt to the development of the immersive world. The results of this study emphasize the urgency of legal reform that is proactive, integrative, and based on digital ethics, so that the law is not only an enforcement instrument but also functions as a means of prevention, education, and protection of individual dignity in the ever-evolving virtual space.

## Acknowledgement

The author expresses sincere gratitude to all individuals and institutions that supported the completion of this study. Appreciation is extended to legal scholars, technology experts, and practitioners who provided valuable insights related to metaverse-based cyber harassment and virtual reality. The author also thanks academic mentors and colleagues for their constructive input. It is hoped that this research contributes to strengthening the legal framework and addressing normative needs in emerging virtual environments.

## References

Adke, V., Bakhshi, P., & Askari, M. (2022). Impact of Disruptive Technologies on Customer

Experience Management In ASEAN: A Review. *2022 IEEE International Conference on Computing (ICOCO)*, 364–368. https://doi.org/10.1109/ICOCO56118.2022.10031882

Al Gazali, M. A. A. G., Kriyantono, R., & Wulandari, M. P. (2023). Situational Perception Correlation Study, Situational Motivation, and Communication Actions in Malang Brawijaya University Students on the Issue of Sexual Harassment in Indonesian Higher Education Environment in 2022. *Technium Social Sciences Journal*, *39*, 234–248. https://doi.org/10.47577/tssj.v39i1.8004

Anshari, M., de Pablos, P. O., & Almunawar, M. N. (2024). Digital health in ASEAN an exploratory analysis. In *Digital Healthcare in Asia and Gulf Region for Healthy Aging and More Inclusive Societies* (pp. 169–198). Elsevier. https://doi.org/10.1016/B978-0-443-23637-2.00021-7

Apriliyanti, I. D., Kusumasari, B., Pramusinto, A., & Setianto, W. A. (2021). Digital divide in ASEAN member states: analyzing the critical factors for successful e-government programs. *Online Information Review*, *45*(2), 440–460. https://doi.org/10.1108/OIR-05-2020-0158

Arifin, R., Riyanto, S., & Putra, A. K. (2023). Collaborative efforts in ASEAN for global asset recovery frameworks to combat corruption in the digital era. *Legality : Jurnal Ilmiah Hukum*, *31*(2), 329–343. https://doi.org/10.22219/ljih.v31i2.29381

Chang, L. Y. C. (2020). Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 327–343). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_6

Chen, X., & Yang, Y. (2022). Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *The International Spectator*, *57*(3), 48–65. https://doi.org/10.1080/03932729.2022.2066841

Chimmanee, K., & Jantavongso, S. (2024). Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN. *Expert Systems with Applications*, *249*, 123652. https://doi.org/10.1016/j.eswa.2024.123652

Chow, Y.-W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and Cybersecurity in the Metaverse: A Survey. *Journal of Imaging*, *9*(1), 11. https://doi.org/10.3390/jimaging9010011

Dincelli, E., & Yayla, A. (2022). Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective. *The Journal of Strategic Information Systems*, *31*(2), 101717. https://doi.org/10.1016/j.jsis.2022.101717

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Farag, N., Ghoniemy, S., & Karam, O. H. (2023). Enhanced Semantic-based Chaotic System for Cyber-grooming Classification and Harassment Detection. *2023 International Conference on Computer and Applications (ICCA)*, 1–10. https://doi.org/10.1109/ICCA59364.2023.10401840

Filia, H. Z., & Setiyono, J. (2024). Sexual Harassment of Women through Social Media in the Modern Era of Indonesian Criminal Law. *International Journal of Social Science and Human Research*, *7*(03). https://doi.org/10.47191/ijsshr/v7-i03-82

Gu, J., Wang, J., Guo, X., Liu, G., Qin, S., & Bi, Z. (2023). A Metaverse-Based Teaching

Building Evacuation Training System With Deep Reinforcement Learning. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2209–2219. https://doi.org/10.1109/TSMC.2022.3231299

Hibatulloh, M. F., & Rasyid, F. (2024). Representation of Sexual Harassment Victims in English-based Indonesian Online News: A Critical Discourse Analysis. *Muslim Education Review*, *3*(2), 431–458. https://doi.org/10.56529/mer.v3i2.322

Huynh-The, T., Pham, Q.-V., Pham, X.-Q., Nguyen, T. T., Han, Z., & Kim, D.-S. (2023). Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence*, *117*, 105581. https://doi.org/10.1016/j.engappai.2022.105581

Hwang, G.-J., & Chien, S.-Y. (2022). Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective. *Computers and Education: Artificial Intelligence*, *3*, 100082. https://doi.org/10.1016/j.caeai.2022.100082

Iqbal, I., Chinanasamy, S., & Faizal, S. (2024). Navigating misogynistic cyber harassment: Impacts and challenges faced by Pakistani female journalists. *SEARCH Journal Media and Communication Research*, *16*(2), 35–64. https://doi.org/10.58946/search-16.2.P4

Jain, A., Roy, D. K., Ayasrah, F. T., William, P., & Kulkarni, S. (2024). Enhancing Metaverse Cybersecurity With Federated Learning. *Global Congress on Emerging Technologies (GCET-2024)*, 254–265. https://doi.org/10.1109/GCET64327.2024.10934363

Jeanice, M., & Chowanda, A. (2025). Deep Learning Algorithms Exploration to Model Toxic Comment Classification. *2025 4th International Conference on Electronics Representation and Algorithm (ICERA)*, 587–592. https://doi.org/10.1109/ICERA66156.2025.11087336

Kuru, K. (2023). MetaOmniCity: Toward Immersive Urban Metaverse Cyberspaces Using Smart City Digital Twins. *IEEE Access*, *11*, 43844–43868. https://doi.org/10.1109/ACCESS.2023.3272890

Li, K., Cui, Y., Li, W., Lv, T., Yuan, X., Li, S., Ni, W., Simsek, M., & Dressler, F. (2023). When Internet of Things Meets Metaverse: Convergence of Physical and Cyber Worlds. *IEEE Internet of Things Journal*, *10*(5), 4148–4173. https://doi.org/10.1109/JIOT.2022.3232845

Mandriyani, S., Wahyuningtyas, N. T., Haikal, M. F., & Ifrani, I. (2024). Child Grooming (Technology-Based Sexual Harassment) in the Context of Indonesian Law. *International Journal of Law, Environment, and Natural Resources*, *4*(1), 91–101. https://doi.org/10.51749/injurlens.v4i1.100

Mourtzis, D., Panopoulos, N., Angelopoulos, J., Wang, B., & Wang, L. (2022). Human centric platforms for personalized value creation in metaverse. *Journal of Manufacturing Systems*, *65*, 653–659. https://doi.org/10.1016/j.jmsy.2022.11.004

Muhammad Mutawali. (2022). Customary Law of Dou Donggo Bima from the Perspective of Islamic and Indonesian Positive Law. *AL-IHKAM: Jurnal Hukum & Pranata Sosial*, *17*(1), 1–27. https://doi.org/10.19105/al-lhkam.v17i1.6007

P. Corning, G. (2022). ASEAN and the Regime Complex for Digital Trade in the Asia-Pacific. *Journal of World Trade*, *56*(Issue 6), 915–938. https://doi.org/10.54648/TRAD2022038

Park, S.-M., & Kim, Y.-G. (2022). A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access*, *10*, 4209–4251. https://doi.org/10.1109/ACCESS.2021.3140175

Pooyandeh, M., Han, K.-J., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences*, *12*(24), 12993. https://doi.org/10.3390/app122412993

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. https://doi.org/10.1016/j.cose.2023.103127

Sari, A. C., Iskandar, K., Prasad, A., Yulistiani, R., Kurniawan, A., Fitriawati, N., Charisma, R. A., & Maulina, A. (2024). Comparative Analysis of LSTM and BiLSTM for Sexual

Harassment Classification on Indonesian Social Media. *2024 7th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 995–1000. https://doi.org/10.1109/ISRITI64779.2024.10963555

Simorangkir, D. N. (2020). Work-related sexual harassment and coping techniques: the case of Indonesian female journalists. *Media Asia*, *47*(1–2), 23–33. https://doi.org/10.1080/01296612.2020.1812175

Suarta, I. M., Suwintana, I. K., Sudiadnyani, I. G. A. O., & Sintadevi, N. P. R. (2024). Employability and digital technology: what skills employers want from accounting workers? *Accounting Education*, *33*(3), 274–295. https://doi.org/10.1080/09639284.2023.2196665

Suhardin, Y., Siahaan, R. H., Sitorus, R., & Amboro, Y. P. (2024). Considering Responsibilities: The Indonesian Government at the Intersect of Environmental Damage and Sustainable Development Goals. *WSEAS TRANSACTIONS ON ENVIRONMENT AND DEVELOPMENT*, *20*, 424–442. https://doi.org/10.37394/232015.2024.20.40

Tendean, M. J. E. (2022). A dramatistic analysis of Indonesian influencers' statements in responding to sexual harassment allegations. *International Journal of Communication and Society*, *4*(2), 235–249. https://doi.org/10.31763/ijcs.v4i2.752

Torres-Parra, C. R., Cuervo-Pulido, R., Flórez-Flórez, J., & Ramírez-Pérez, O. (2022). Diseño participativo como método para la creación de videojuegos críticos. Poder Violeta, estudio de caso de un videojuego sobre acoso sexual. *Revista Colombiana de Educación*, *85*, 1–26. https://doi.org/10.17227/rce.num85-12568

Ulubas-Varpula, I. Z., & Björkqvist, K. (2021). Peer Aggression and Sexual Harassment among Young Adolescents in a School Context: A Comparative Study between Finland and Turkey. *International Journal of Educational Psychology*, *10*(3), 199–221. https://doi.org/10.17583/ijep.6853

Wang, C.-N., Nhieu, N.-L., & Liu, W.-L. (2024). Unveiling the landscape of Fintech in ASEAN: assessing development, regulations, and economic implications by decision-making approach. *Humanities and Social Sciences Communications*, *11*(1), 100. https://doi.org/10.1057/s41599-023-02581-2

Wang, H., Ning, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2023). A Survey on the Metaverse: The State-of-the-Art, Technologies, Applications, and Challenges. *IEEE Internet of Things Journal*, *10*(16), 14671–14688. https://doi.org/10.1109/JIOT.2023.3278329

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials*, *25*(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

Zhang, X., Chen, Y., Hu, L., & Wang, Y. (2022). The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.1016300