Journal of Sharia and Legal Science
Vol. 4 No. 1 April 2026, 1 - 17
Publisher: CV. Doki Course and Training
E-ISSN: 2987-601X P-ISSN: 2988-7119
DOI:https://doi.org/10.61994/jsls.v4i1.1679

Metacrime and Online Deviance: Law Enforcement Complexities in the Metaverse Era

Henky Fernando[1*], Yuniar Galuh Larasati[2]
Faculty of Cultural Sciences, Universitas Gadjah Mada[1,2]
Corresponding email: fhenky92@gmail.com

Abstract:
Law enforcement in the metaverse era has placed authorities and policymakers in increasingly complex challenges of prevention and enforcement. While existing studies offer valuable insights, they remain limited in addressing the emerging dynamics of crime within conventional digital environments. In addition to addressing the limitations of existing studies, this research aims to explain the characteristics of online crime and deviant behavior in the Metaverse and their implications for law enforcement practices. This study adopts a qualitative descriptive approach grounded in multimodal ethnography to elucidate the patterns, operational modalities, and forms of impact that emerge within immersive environments. The key findings indicate that crime in the Metaverse not only transcends the characteristics of conventional violations but also generates more complex forms of symbolic, psychological, and virtual economic harm. Anonymity, cross-jurisdictional interactions, and avatar-mediated engagement further complicate the attribution of legal responsibility. In other words, the transformation of digital spaces necessitates more responsive regulatory adaptation to ensure effective legal protection. The significance of this study lies in its contribution as a conceptual foundation for the development of policies and law enforcement strategies in the metaverse era.

Keywords: *metacrime; online deviance; law enforcement; metaverse era*

Introduction

In the era of the Metaverse, law enforcement faces complexities that extend beyond prevention to include the normative handling of moral violations within immersive environments. The character of interactions based on avatars, anonymity, and cross-jurisdictional connectivity increasingly blurs the boundary between symbolic actions and their real-world consequences (Kang & Rhee, 2025). According to Tiwari et al. (2025), in addition to the growing diversity of modes and motives, the definitions of victims and perpetrators have become problematic because digital identities can be engineered, duplicated, or disguised, thereby complicating the attribution of legal responsibility. Metacrime and other forms of online deviance in the Metaverse also exhibit significant differences in psychological impact, virtual economic losses, and the intensity of immersive experiences perceived by victims (Zhou et al., 2024). The complexity of law enforcement in the metaverse era, therefore, needs to be explained through an interdisciplinary approach that integrates cyber law and digital criminology. Such an approach is essential to ensure that legal systems can respond to evolving forms of violations proportionately and adaptively in the metaverse era.

The distinctive characteristics of metaverse-based online crime and deviance, compared with conventional crime, can be explained through the concepts of cybercrime and space transition theory, which emphasise ontologically distinct interaction structures (Martha, 2024; Zhou et al., 2024). Within the context of the Metaverse, crime is no longer

dependent on geographical proximity; rather, it is shaped by network connectivity and avatar-mediated interactions that enable offenders to manipulate their identities (Kuznetsova et al., 2025). While conventional crimes are generally based on direct contact and material evidence, activities in the Metaverse are often symbolic and immersive, leaving complex digital traces. According to XinYing et al. (2024), social deviance in the Metaverse also tends to occur within virtual community spaces whose norms and sanctioning mechanisms are not yet firmly established, thereby blurring the boundary between deviant behavior and creative expression. These characteristics indicate that metaverse-based crime has a more complex dimension, particularly in its prevention.

Preventing crime in the Metaverse requires an approach that differs from conventional strategies, which generally rely on physical control, patrols, and repressive enforcement. Tilley & Sidebottom (2014) emphasise the importance of environmental engineering to reduce opportunities for crime. However, in the context of the Metaverse, the "environment" takes the form of digital architecture, algorithms, and interaction design. The routine activity approach must also be reinterpreted, as the convergence of offender, target, and the absence of a capable guardian now occurs within virtual spaces that are not bound by geographical limitations (Chawki et al., 2024; Leukfeldt & Yar, 2016). While conventional crimes can often be prevented through the physical presence of law enforcement, crime prevention in the Metaverse requires integrating safety-by-design principles, AI–based moderation, and user digital literacy. The complexity of law enforcement in the metaverse era is therefore crucial to examine in order to formulate regulatory and preventive models that are adaptive and responsive to the continuously evolving dynamics of digital crime.

Over the past five years, studies addressing law enforcement issues in the digital era have tended to adopt a normative orientation and have largely focused on three dominant themes. First, studies that examine harmonization of regulations and reform of cyber legal frameworks to accommodate technological developments (AllahRakha, 2024; Febriansyah et al., 2026; Fekolli et al., 2025). Second, studies that analyze aspects of personal data protection and information security as the foundation of legal legitimacy in digital spaces (Abouahmed et al., 2024; Kalashnikova, 2022; Sepulveda et al., 2025). Third, studies that evaluate the effectiveness of law enforcement in addressing transnational cybercrime, including challenges related to jurisdiction and international cooperation (Cao & Vu, 2025; Magableh & Al-Shawabkeh, 2024; Setiyawan et al., 2024). These three themes indicate that the approaches employed in existing studies remain largely structural and normative. Meanwhile, the immersive and social dynamics within the metaverse environment have not yet been comprehensively and contextually explored and, in many cases, have been overlooked.

The aim of this study is not only to address the limitations of previous studies but also to analyze the characteristics of online crime and deviant behavior in the Metaverse. This focus is important because the Metaverse has introduced a configuration of immersive

interactions based on avatars and cross-jurisdictional engagement, meaning that the patterns of violations that emerge cannot be fully explained through conventional cybercrime frameworks. Dwivedi et al. (2023) argue that, in addition to their complex characteristics, online crime and deviance in the Metaverse also carry latent implications that differ from conventional violations, particularly in terms of psychological impacts, identity construction, and forms of symbolic and virtual economic harm. This phenomenon requires an analytical perspective that goes beyond legal-formal interpretations and incorporates sociological and criminological approaches. In other words, this study seeks to contribute to the academic discourse by presenting an analysis that is contextual and responsive to the evolving dynamics of law enforcement.

Online crime and deviant behavior emerging in the metaverse arena constitute a critical phenomenon to be examined to evaluate law enforcement's challenges in immersive digital spaces. The Metaverse not only expands forms of social interaction but also reconfigures patterns of violations through avatar anonymity and cross-jurisdictional relations. In explaining this phenomenon, this study focuses on three main questions. First, what are the characteristics of crimes that occur frequently in the Metaverse? Second, what forms of potential online deviance emerge within the dynamics of virtual communities? Third, what are the implications of such crimes and deviant behaviors for the effectiveness and adaptability of law enforcement? This study is also grounded in the argument that crime and deviance in the Metaverse not only exhibit characteristics that extend beyond conventional violations but also generate more complex forms of symbolic harm. In other words, immersive crime and deviance in the Metaverse transcend both the characteristics and implications of conventional cybercrime.

Method

This study selects the phenomenon of online crime and deviance as its primary unit of analysis, as both represent the most evident forms of social transformation within the immersive and symbolically interactive ecosystem of the Metaverse. Crime and deviance are no longer merely extensions of conventional online practices; rather, they have intensified through the use of avatars, virtual economies, and complex cross-jurisdictional relations. This phenomenon is academically significant because it demonstrates a shift in the locus delicti, forms of harm, and constructions of victimhood that are not fully accommodated within existing positive legal frameworks. In this study, the Metaverse is positioned not only as a technological innovation but also as a social arena that generates new forms of risk. Reflecting on the challenges of law enforcement in the metaverse era is therefore essential, as its anonymous, transnational, and platform-based characteristics require more adaptive regulatory approaches. Accordingly, this study seeks to address the gap between the evolving dynamics of digital crime and the capacity of legal systems in the metaverse era.

This study employs a qualitative descriptive research design grounded in multimodal ethnography, as this approach facilitates an in-depth examination of the dynamics of online crime and deviance within the context of the metaverse. The qualitative approach is selected to understand patterns of interaction and the social constructions underlying particular events, rather than merely measuring the frequency or statistical occurrence of incidents. The case study model provides a space for contextual analysis of specific events that represent the complexity of relationships among technology, users, and regulatory frameworks. This study also uses online media reports as the primary data source, as they provide documented records of publicly reported events, including incident chronologies, platform responses, and reactions from authorities. Online media also function as a medium that reflects how particular cases are understood and framed within the digital public sphere. These data sources are therefore relevant for mapping patterns, identifying dominant issues, and analyzing the social narratives that develop around crime and deviance in the Metaverse.

The data collection process involved observing online news articles reporting cases of crime and deviant behavior in the Metaverse. Data retrieval was carried out using the Google search engine with the keyword “crime and deviance in the metaverse” to identify relevant, recent news reports that provided adequate descriptions of the events. The observation focused on identifying patterns of modus operandi, forms of deviance, platform responses, and the legal implications emerging from each case. Each news report was carefully reviewed, categorized by violation type and analyzed to capture recurring conceptual themes. Data saturation was considered reached when no further significant variation was observed in case patterns, motives, or media-reported responses. Online news documents were also treated as publicly available secondary sources and analyzed, with proper citations and content integrity preserved, in accordance with the principles of scientific ethics and academic responsibility.

Data analysis in this study was conducted in three stages, as proposed by Miles and Huberman (1994): data reduction, data display, and conclusion drawing/verification. In the data reduction stage, the researcher selected, focused on, and simplified information from online news documents relevant to the theme of crime and deviance in the Metaverse, retaining only data with substantive relevance. The next stage was data display, in which the reduced findings were systematically organized into thematic categories, patterns of modus operandi, and forms of legal and platform responses, enabling a more comprehensive understanding of the relationships among variables. The final stage involved conclusion drawing and verification, which consisted of interpreting meanings based on the emerging patterns while simultaneously examining the consistency of the findings with the theoretical framework employed in the study. These three stages were conducted interactively and iteratively to ensure that the analysis remained logical, structured, and capable of comprehensively representing the complexity of online crime and deviant behavior within the Metaverse.

Results and Discussion

Massive Crime Occurring within the Metaverse Arena

The Metaverse, as an arena of expressive and creative social communication, also has the potential to configure opportunities for crime through the mobility of interactions that transcend physical and geographical boundaries. Melis & Monaro (2025) argue that crime in the metaverse era no longer depends on physical encounters, but rather on symbolic access to digital self-representations mediated through immersive experiences. The immersion enabled by digital technologies has expanded the definition of victimization into the representational realm, meaning that violations against users' avatars in the Metaverse cannot simply be reduced to normal simulations. Virtual sexual harassment exemplifies how relations of power and aggression can be manifested through digital bodies that function as extensions of users' subjectivity. This phenomenon can be illustrated by a report from Berlin (2022) stating that a female metaverse user reported experiencing sexual harassment, in which her avatar was groped and harassed by several other avatars in a virtual space. This case demonstrates that sexual aggression can occur within immersive forms of interaction in the metaverse arena, thereby surpassing the conceptual boundaries of conventional normative protection.

Within the Metaverse, spaces of interaction can be understood as dialogical fields between the potential for creative expression and the possibility of victimization, both produced by the structure of its communication. Narayanan et al. (2020) argue that technological mediation, sensory immersion, and avatar anonymity have created conditions that loosen normative engagement with the physical body, such that virtual social actions are no longer associated with collective moral responsibility. This condition is not merely a matter of individuals failing to adapt to the security features of the Metaverse, but rather a structural consequence of a communication architecture that facilitates affective distance between perpetrators and victims of virtual crime. Valera et al. (2026) state that the Metaverse is often treated as a space of symbolic representation, leading to experiences of crime being reduced to actions perceived as unreal, even though phenomenologically, such actions still disrupt personal integrity and the sense of security. In other words, the Metaverse cannot be understood as a neutral space; rather, it should be viewed as a social arena that produces ambiguity between simulation and lived experience.

The characteristics of crimes that frequently emerge in the Metaverse are also manifested through digital economic manipulation that exploits users' speculative expectations for virtual assets. According to Wiwoho et al. (2021), such actions result from a shift in the structure of trust toward symbolic representations produced through virtual communication. This pattern can be observed in metaverse-based investment promotions positioned as opportunities for digital capital accumulation, such as the NTF-Metaverse platform, which offers profits from NFT trading and virtual land ownership but demonstrates manipulative characteristics through profit-sharing claims that are difficult to verify (Jayenadmin, 2025). Patterns of crime, such as fraud, in the Metaverse often reproduce

manipulative logics derived from offline crypto-based schemes, which are further expanded through immersive experiences that construct perceptions of credibility and authenticity in risk-related interactions. Fraudulent activities in the Metaverse indicate that cybercrime practices do not always originate in technological innovation itself, but rather in mediated patterns of public communication that continue to evolve through processes of mediatisation.

Communication schemes within the metaverse environment reveal tensions between the acceleration of technological innovation and the adaptation of legal regulation, thereby creating opportunities for complex forms of digital crime. Zhou et al. (2024) conceptualise this phenomenon as metacrime, because the crimes that emerge cannot be understood as simple extensions of conventional cybercrime practices but rather as practices that operate through configurations of virtual identity. This condition can be illustrated by reports of major data breaches in Indonesia, such as the 2025 attack on the BPJS Kesehatan participant data system, which exposed millions of users' private data to the public. The incident demonstrates how the structure of digital platforms can become highly vulnerable targets for criminal activities that are difficult to trace effectively (Unesa, 2025). Thus, communication schemes within the metaverse environment are not merely spaces for creative interaction, but also socio-technological configurations that challenge the conceptual boundaries of moral norms and the authority of legal frameworks in responding to the evolving dynamics of crime in the metaverse era.

Criminal practices within the metaverse arena have evolved massively, extending beyond the normative logic of law, as reflected in the linear continuation of cybercrime that has shifted toward metacrime, operating within the complexity of digital platform realities. Whereas cybercrime was previously understood through frameworks of illegal access, data manipulation, or network violations, metacrime instead re-examines the ontological foundations of responsibility when identity, ownership, and presence are mediated through avatar-based representations (Tiwari et al., 2025). Hyper-digital spatiality and representational ownership have created a communicative arena in the Metaverse that does not fully align with the normative logic of positive law, thereby rendering the definitions of offender, victim, and locus delicti subjects of epistemic negotiation. Kuznetsova et al. (2025) note that legal systems tend to operate reactively, while innovations in virtual communication evolve at an accelerated pace, creating an asynchrony that opens opportunities for criminal activity within these normative gaps. In other words, metacrime does not merely refer to a new type of violation, but signals a broader transformation in the modes and motives of virtual crime.

Massive criminal activity within the metaverse exerts significant implications for law enforcement processes, as conventional legal systems remain insufficiently equipped to address the complexity of avatar-based social spaces and immersive interactions. Fernando & Larasati (2026) Law enforcement is no longer confronted solely with issues of evidentiary proof of criminal acts, but also with epistemological challenges concerning the definition of victims and perpetrators, the determination of locus delicti, and the validity of virtual

experiences as forms of tangible harm. The anonymous and transboundary character of the metaverse further complicates the identification of offenders, rendering investigations more intricate than in conventional cybercrime contexts. This condition is exacerbated by rapid technological innovation that is not matched by regulatory adaptation, resulting in a predominantly reactive legal framework, while patterns of virtual criminality evolve dynamically and transnationally, surpassing the institutional monitoring capacity of the state.

Criminal activities within the metaverse arena demonstrate increasingly complex modes and motives, as they enable the transformation of crime into more manipulative and less detectable forms. González-Tapia (2023) Criminal modus operandi are no longer confined to data theft or unauthorized access, but have expanded to include the exploitation of avatar identities, affective manipulation through immersive experiences, and the construction of virtual social spaces for collective fraud based on digital economies. The motives of offenders are likewise broadening, extending beyond financial gain to encompass symbolic domination, psychological exploitation, and the production of fear within virtual environments. This complexity arises from the metaverse's capacity to generate ambiguity between simulation and social reality, allowing perpetrators to reproduce forms of violence or manipulation without necessarily perceiving themselves as bound by conventional moral responsibility.

Potential Online Deviance in the Metaverse Arena

Social interaction within the metaverse arena is not only imagined as an extension of collective creativity but also creates structural conditions that allow the emergence of trolling as a form of interactional deviance. Avatar anonymity and the flexibility of digital identity tend to reduce personal accountability while simultaneously reconfiguring the boundary between symbolic performativity and social consequences. As a result, verbal aggression is often produced and normalized as a communicative practice (Webb, 2001). In this context, trolling does not merely reflect individual intentions but is rooted in the configuration of virtual spaces that create affective distance and weaken normative sanctions. Online media reports concerning alleged verbal harassment and offensive behavior on virtual reality platforms such as Horizon Worlds owned by Meta Platforms illustrate how degrading speech and interactive disturbances increasingly occur within users' immersive experiences (France-Presse, 2022). These conditions affirm that communication dynamics in the Metaverse are vulnerable to deviant practices, not as incidental anomalies but as consequences of the structural characteristics of digital communication.

From the perspective of social interaction, the metaverse arena functions not merely as a space for message exchange but as a field for the dynamic negotiation of social positions. The flexibility of digital identities encourages individuals to perform their self-image, such that symbolic interactions often produce moral tensions when the boundary between expression and norm violation blurs (Sharma et al., 2025). Open access to creativity and collaboration expands participation, yet it simultaneously forms loose social networks that are not always accompanied by strong community attachment. When social cohesion

weakens, normative sanctions lose their resonance and social control becomes less effective (Yang et al., 2025). According to Zhou et al. (2024), these conditions render practices of symbolic provocation and conflict play as structural phenomena that have the potential to evolve into latent forms of metacrime. In other words, the metaverse arena contains the potential for the large-scale reproduction of online deviance, as its interactional space is shaped by the simultaneous dialectics of digital communication, thereby increasing the risk of the normalization of deviant behavior.

Aggressiveness and provocative interaction in the Metaverse can be understood as deviant conversations grounded in visibility, recognition, and the distribution of symbolic power, rather than merely as personal disruptions. Provocative practices function as a performative language for negotiating positions within the digital hierarchy, in which the emotional responses of audiences become a medium for the production and circulation of shared meaning (Fernando, Larasati, Abdullah, et al., 2025; Larasati et al., 2026). Sideris (2011) also argues that empathy does not entirely disappear; rather, it is renegotiated within the boundaries of avatar representation and community norms, allowing antagonism to appear as a legitimate expression in certain situations. The repetition of such practices gradually establishes a normative dialogue that shifts community perceptions of conflict, transforming it into an institutionalized style of communication. Online deviance not only generates relational tensions but also challenges authority in determining meaning and legitimate interaction boundaries (Denegri-Knott & Taylor, 2005). In other words, potential deviance in the Metaverse emerges not merely as symbolic dialogue but as a mechanism of recognition exchange that reconstructs the landscape of digital social relations.

The Metaverse has created configurations of interaction that expand social experiences while simultaneously opening spaces for sexual deviance operating through the symbolic representation of digital bodies. Such practices are distributed in the form of explicit content, non-consensual role-playing, and the formation of communities with exploitative orientations. They therefore cannot be understood merely as individual deviations (Ojha & Vaish, 2025). Mediation through avatars reduces affective relations to objects of representational manipulation, allowing violations of personal integrity to occur without physical contact while still producing tangible psychological impacts. This phenomenon can be illustrated by reports from Bates (2025) concerning alleged sexual harassment on virtual reality platforms such as Horizon Worlds, where users reported experiencing unwanted virtual touching and repeated sexual comments within immersive environments. These phenomena confirm that sexual deviance in the Metaverse is not simply an anomaly but rather a consequence of the dialectic between technological design and the evolving flexibility of virtual identities.

The potential for sexual norm deviance in the Metaverse can be understood as a latent dialogue between technological structures and psychosocial self-regulation, rather than merely a matter of weak individual control. When avatars and digital distance mediate interaction, subjectivity negotiates with conditions of invisibility that relativize social

consequences (Roth et al., 2019). Anonymity, asynchronous responses, and symbolic immersion create a dialogical situation in which experiences of presence test empathy without a physical body. In this context, victims may still experience affective intrusion, as virtual proximity can activate genuine emotional responses, indicating that social experience is not entirely determined by materiality (Kim et al., 2025). Communication disinhibition in the metaverse era not only loosens social control but also transforms the meaning relationships among courage, vulnerability, and responsibility in interaction. The Metaverse has thus become a symbolic space where freedom of expression and ethical boundaries are continuously negotiated, such that understanding virtual norms requires viewing them as collective constructions of meaning in digital social interaction.

Deviant interactions within the metaverse exert significant implications for normative morality, as the boundaries between digital expression, symbolic aggression, and ethical transgression become increasingly blurred within immersive virtual communication spaces. The anonymity of avatars and the fluidity of digital identity contribute to a weakening of personal moral responsibility (Azhar et al., 2026; Hidayat et al., 2026; Zhou et al., 2024), whereby practices such as trolling, verbal harassment, and symbolic provocation are gradually reproduced as normalized forms of communication. In this context, normative morality no longer operates as a stable set of collective values, but is continuously renegotiated in accordance with the dynamics of digital culture and the logic of social performativity. As audience emotional responses become a source of recognition and symbolic power, communicative aggression may acquire social legitimacy as part of community interaction styles. Consequently, empathy is not entirely diminished, but rather reduced to the level of avatar-based representation, which remains relatively detached from the tangible social consequences of digital interactions.

Deviant behavior within the metaverse arena also demonstrates considerable complexity in both its modes and motives, as the structure of virtual interaction enables deviance to be reproduced through the interplay of anonymity and symbolic immersion. Melis & Monaro (2025) argues the modalities of deviance are no longer limited to trolling or basic verbal harassment, but may extend to avatar-based psychological manipulation, virtual sexual exploitation, the formation of concealed deviant communities, and the simulation of social relationships within metaverse environments. The motives of actors likewise expand beyond mere entertainment or provocation toward the pursuit of social recognition, the distribution of symbolic power, affective exploitation, and the construction of alternative digital identities that gain legitimacy within virtual communities. This complexity emerges from the metaverse's capacity to create a dialogical condition between expressive freedom and weak social control, allowing deviance to manifest as a form of interaction that is perceived as normative.

Challenges of Law Enforcement in the Metaverse Era

The modus operandi of crime and online deviance within the metaverse environment has evolved through the exploitation of structural gaps in immersive technologies that have

not yet been fully accommodated within conventional legal frameworks (Fernando & Larasati, 2022). Offenders may manipulate digital identities, infiltrate private virtual spaces, exploit affective relationships through virtual grooming, and even engineer immersive experiences to create psychological pressure without direct physical contact. Practices such as the seizure of digital assets, extortion based on recordings of virtual interactions, and the misuse of biometric data from VR devices illustrate forms of crime operating at the intersection between physical reality and symbolic representation. The underlying motives are not solely economic but also include the pursuit of status, symbolic dominance, existential gratification, and the exploration of power within spaces characterized by minimal accountability (Bourdieu, 1986). However, legal regulations often remain focused on material objects and territorial jurisdiction. As a result, such actions frequently fall within a normative grey area, as the metaverse environment enables deviant innovation and criminal practices to evolve more rapidly than the state's regulatory responses.

Challenges to law enforcement in the metaverse environment arise because its interactional structure transcends the boundaries of territorial jurisdiction, legal identity, and the conventional definition of legal objects based on materiality (Qin et al., 2025). Offenders and victims may be located in different countries, operate under avatar identities separate from their civil identities, and conduct transactions using digital assets that may lack a clearly defined legal status. The process of proving such cases also becomes complex, as evidence may take the form of recordings of virtual interactions, cross-border server data, or digital traces controlled by platform corporations. Consequently, law enforcement agencies often depend on international cooperation and the private policies of technology companies. Pandey (2025) notes that the absence of clear classifications of symbolic violence, virtual harassment, or the seizure of digital assets across several national legal systems has created normative gaps that complicate criminalisation. In other words, law enforcement in the metaverse era faces structural challenges characterized by anonymity and regulatory lag amid the rapid acceleration of digital technological innovation.

In theories of law enforcement and crime prevention, cases of norm violations within the metaverse arena can be explained through the perspectives of deterrence theory and Situational Crime Prevention. Clarke (1980) argues that Deterrence Theory emphasizes that crime can be reduced when there is certainty, swiftness, and proportionality in sanctions, thereby encouraging potential offenders to consider the risks before acting. However, in the anonymous, cross-jurisdictional environment of the Metaverse, deterrent effects can be effective only when supported by digital identification mechanisms and cross-national regulatory collaboration. Freilich (2015) also notes that the situational crime prevention approach focuses on reducing opportunities for crime by designing secure environments, such as strengthening moderation systems, restricting certain forms of interaction, and implementing responsive reporting mechanisms. Nevertheless, the metaverse arena does not merely function as a service provider but also acts as a regulatory actor that shapes the architecture of digital social control. The integration of these two theoretical perspectives

indicates that law enforcement in the metaverse era must combine formal sanctions with technological design engineering to minimize the rationalization of deviant behavior.

If law enforcement fails to respond to and address crime and online deviance within the metaverse environment, the implications extend beyond an increase in the frequency of violations to the normalization of deviance as part of digital interaction culture. The absence of an effective regulatory response may reinforce perceptions of impunity, encouraging offenders to develop increasingly complex modus operandi while simultaneously weakening users' sense of security and trust in the virtual ecosystem. According to Effing & Hinz (2024), such conditions may potentially create digital segregation, in which vulnerable groups withdraw from participation due to the risks of harassment or exploitation. As a result, the metaverse space may be dominated by aggressive, opportunistic actors. The failure of regulation can also shift collective ethical standards, allowing symbolic violence, identity manipulation, and affective exploitation to become practices that are perceived as normal within the metaverse arena. The accumulation of these conditions not only disrupts the governance of virtual spaces but also affects the broader social order, as the boundaries between digital reality and everyday social life become increasingly blurred (Scott, 2023).

Given that the latent dangers of crime and online deviance in the metaverse environment do not always manifest as explicit violations, this study recommends strengthening adaptive, responsive regulatory frameworks that account for the immersive, anonymous, and cross-jurisdictional characteristics of virtual interactions. Regulations need to expand the definition of legal objects to include symbolic violence, avatar-based harassment, and the exploitation of digital assets and data as forms of violations that carry real consequences. Hine (2023) also argues that collaboration among states, platform providers, and user communities is crucial to establishing transparent and accountable law-enforcement mechanisms in the metaverse era. The safety-by-design approach should also be integrated through privacy protections, restrictions on high-risk interactions, and effective reporting systems for victims. Accordingly, the governance of the Metaverse should be directed toward a collaborative regulatory model that is not only reactive to violations but also preventive in shaping a digital ecosystem that is safe, ethical, and sustainable.

Online crime and deviance within the metaverse environment exhibit fundamental differences from conventional digital crime. Whereas traditional cybercrime typically centers on data theft, network intrusion, or transaction-based fraud, metaverse-based criminality extends further by exploiting avatars, virtual spaces, affective relations, and users' psychological experiences as objects of victimization. Practices such as virtual grooming, symbolic intimidation, the exploitation of avatar interactions, and the misuse of VR biometric data indicate that victimization in the metaverse is not solely material, but also implicates users' emotional integrity and representational identity (Tschanter et al., 2026). The motives of perpetrators are likewise more complex, encompassing not only economic interests but also the pursuit of symbolic domination, social existence, recognition within virtual communities, and the exploration of power within anonymous environments

characterized by weak social control (Fernando, Larasati, Barkah, et al., 2025; Larasati et al., 2025).

Law enforcement in the metaverse era faces challenges far more complex than those associated with other forms of digital crime, as evidentiary processes must contend with anonymous avatar identities that lack clear normative classification. In the context of conventional cybercrime, evidentiary standards generally remain oriented toward material digital traces, such as system access logs, electronic transactions, or network data (Antwi, 2025). In contrast, evidence in the metaverse may take the form of recorded virtual interactions, victims' immersive experiences, the manipulation of digital environments, or symbolic exploitation elements that are difficult to verify within existing legal frameworks. Furthermore, the motives and modalities of metaverse-based crime, which are rooted in psychological experience and symbolic domination, often render conventional legal approaches insufficient to adequately articulate the forms of harm experienced by victims. This condition underscores the need for a new regulatory approach to law enforcement in the metaverse era one that integrates technological capacity with a nuanced understanding of virtual social relations.

Conclusion

In the metaverse era, crime and online deviant behavior have undergone an immersive transformation that simultaneously affects the conception of both offenders and victims. The characteristics of crimes emerging within the metaverse arena are not only symbolically immersive but also produce tangible psychological, reputational, and economic impacts on users. Interactions mediated through metaverse representations have increasingly blurred the boundary between symbolic experiences and real social consequences. In addition, online deviant practices have significant potential to occur due to the ambiguity of identity and the absence of clear geographical boundaries, which complicate tracking and legal accountability. Anonymity conditions and the limited presence of normative control further expand opportunities for manipulation, exploitation, and symbolic aggression in virtual spaces. The development of such crimes and deviant behaviors not only indicates the adaptation of deviant conduct to technological innovation but also poses serious challenges for the establishment of proportional and effective systems of crime prevention and law enforcement.

The findings of this study can serve as a dialogical foundation for the development of conceptual discourse in legal and criminological studies, particularly in responding to the transformation of crime within immersive digital spaces such as the Metaverse. Changes in interaction, identity, and legal objects indicate that conventional normative approaches are no longer entirely sufficient to explain patterns of deviance involving avatars, virtual assets, and symbolic relations. Therefore, this study opens space for theoretical reflection on the expansion of the definitions of victims, offenders, and forms of harm that are not always material in nature but may produce psychosocial and reputational impacts. In addition, the findings of this study encourage integrating perspectives from digital criminology,

mediation theory, and transnational regulation to develop a more adaptive analytical framework. Such conceptual dialogue is important to ensure that legal frameworks do not lag behind technological developments, while also ensuring that the principles of justice and the protection of rights remain relevant within rapidly evolving, increasingly complex virtual social ecosystems.

This study also has limitations in the data collection process, as it relies solely on online news reports as the primary source of analysis. Consequently, the data obtained and interpreted are limited to constructions of events that have undergone selection and framing processes and therefore do not fully represent the direct experiences of victims, offenders, or the internal dynamics of metaverse platforms. This reliance on such sources has also limited the depth of exploration regarding motives, patterns of interaction, and broader structural contexts. Nevertheless, these limitations may serve as an important foundation for future research to develop more comprehensive methodological approaches, such as in-depth interviews, virtual participant observation, or platform policy analysis. By expanding both data sources and data collection techniques, future studies are expected to yield a more empirical, multidimensional understanding of crime and social deviance in the Metaverse.

References

Abouahmed, A., Kandeel, M. E., & Zakaria, A. (2024). Personal data protection in the United Arab Emirates and the European Union regulations. *Journal of Governance and Regulation*, *13*(1), 195–202. https://doi.org/10.22495/jgrv13i1art17

AllahRakha, N. (2024). Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds. *Lex Scientia Law Review*, *8*(1), 405–432. https://doi.org/10.15294/lslr.v8i1.2081

Antwi, N. (2025). Forensic Artifacts in Operating Systems Windows vs. Linux. In *Leveraging Large Language Models for Quantum-Aware Cybersecurity* (pp. 169–200). https://doi.org/10.4018/979-8-3373-1102-9.ch006

Azhar, R., Rifmayanti, C., Siregar, R. A., Harahap, A. R., & Ikhsan, M. (2026). The Paradox of Religiosity: Corruption Practices in Islamic Faith-Based Organizations. *Criminology & Islamic Law*, *1*(1), 1–17. https://journal.postinsti.com/index.php/cil/article/view/1

Bates, L. (2025). Misogyny in the metaverse: is Mark Zuckerberg's dream world a no-go area for women? *Guardian*. https://www.theguardian.com/society/2025/jun/10/the-misogyny-of-the-metaverse-is-mark-zuckerbergs-dream-world-a-no-go-area-for-women

Berlin, S. (2022, January 31). Mother Alleges She Was Virtually Groped in Attack Inside Facebook's Metaverse. *Newsweek*. https://www.newsweek.com/mother-alleged-she-was-virtually-groped-attack-inside-facebooks-metaverse-1674718

Bourdieu, P. (1986). The Forms of Capital. In *Handbook of Theory and Research for the Sociology of Education* (pp. 241–258). https://www.researchgate.net/publication/285376612_The_Forms_of_Capital

Cao, O. T., & Vu, T. Van. (2025). Insoluble Challenges of Prosecuting Transnational

Cybercrime: A Case in a Developing Country. *Journal of Forensic Medicine Science and Law*, *34*(1), 60–63. https://doi.org/10.59988/jfmsl.vol.34issue1.12

Chawki, M., Basu, S., & Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, *13*(3), 33. https://doi.org/10.3390/laws13030033

Clarke, R. V. G. (1980). Situational Crime Prevention: Theory and Practice. *The British Journal of Criminology*, *20*(2), 136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Denegri-Knott, J., & Taylor, J. (2005). The Labeling Game: A Conceptual Exploration of Deviance on the Internet. *Social Science Computer Review*, *23*(1), 93–107. https://doi.org/10.1177/0894439304271541

Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., Koohang, A., Ribeiro-Navarrete, S., Belei, N., Balakrishnan, J., Basu, S., Behl, A., Davies, G. H., Dutot, V., Dwivedi, R., Evans, L., Felix, R., Foster-Fletcher, R., Giannakis, M., … Yan, M. (2023). Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. *Information Systems Frontiers*, *25*(5), 2071–2114. https://doi.org/10.1007/s10796-023-10400-x

Effing, R., & Hinz, M. (2024). Are Children Ready for the Metaverse? The Minefield of Virtual Participation in Digital Social Spaces with Harmful Content and Behavior. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1–15. https://doi.org/10.1007/978-3-031-70804-6_1

Febriansyah, F. I., Ikhwan, A., Firdausi, U. S., & Anggoro, A. D. (2026). Digital Legal Transformation: Legal Strategies for Strengthening National Cybersecurity. *International Journal of Law and Society*, *5*(1), 26–44. https://doi.org/10.59683/ijls.v5i1.357

Fekolli, S., Çela, E., Erdolatov, C., Biyashev, B., & Ismailova, G. (2025). Analysis of the Impact of Digital Transformation of the Legal Field on Data Cybersecurity. *Revista de Direito, Estado e Telecomunicacoes*, *17*(2), 1–33. https://doi.org/10.26512/lstr.v17i2.56766

Fernando, H., & Larasati, Y. G. (2022). Metaverse and Hajj: The Meaning of Muslims in Indonesia. *Kuriositas Media Komunikasi Sosial Dan Keagamaan*, *15*(2), 195–217. https://doi.org/https://doi.org/10.35905/kur.v15i2.2622

Fernando, H., & Larasati, Y. G. (2026). AI-Enabled Symbolic Violence Against Muslims: Protecting Honor in Islamic Law. *Criminology & Islamic Law*, *1*(1), 18–35. https://journal.postinsti.com/index.php/cil/article/view/2%0A

Fernando, H., Larasati, Y. G., Abdullah, I., Florika, V. T., & Liyana, C. I. (2025). The Deconstruction of Women ' s Values in # MeToo on Instagram. *Italian Sociologial Review*, *15*(January), 27–46. https://doi.org/10.13136/isr.v15i1.821

Fernando, H., Larasati, Y. G., Barkah, Q., Andriyani, & Morin, L. (2025). Religion in the Metaverse Scheme: Practices of Worship in the New Media Age. *ESENSIA: Jurnal Ilmu-Ilmu Ushuluddin*, *26*(1), 12–26. https://doi.org/10.14421/esensia.v26i1.6445

France-Presse, A. (2022, February 5). Meta adds “personal boundary” tool to virtual world after harassment reports. *Times of Malta*. https://timesofmalta.com/article/meta-adds-personal-boundary-tool-to-virtual-world-after-harassment.932476

Freilich, J. D. (2015). Beccaria and Situational Crime Prevention. *Criminal Justice Review*,

40(2), 131–150. https://doi.org/10.1177/0734016814550815

González-Tapia, M. I. (2023). Virtual emotions and Criminal Law. *Frontiers in Psychology*, *14*. https://doi.org/10.3389/fpsyg.2023.1260425

Hidayat, R., Julkarnaen, Hakim, M. L., Lestari, S. D., & Suratman, B. (2026). Challenges in Enforcing Islamic Law on the Misuse of Ummah Philanthropic Funds. *Criminology & Islamic Law*, *1*(1), 36–51. https://journal.postinsti.com/index.php/cil/article/view/3

Hine, E. (2023). Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression. *Philosophy & Technology*, *36*(3), 43. https://doi.org/10.1007/s13347-023-00645-4

Jayenadmin. (2025, October 27). NFT-Metaverse.online Scam -Fake Metaverse Investment Platform. *Jayen Consulting*. https://jayen-consulting.com/2025/10/27/nft-metaverse-online-scam-fake-metaverse-investment-platform/

Kalashnikova, E. B. (2022). Personal Data Protection as a Basis of Digitalization. In *Lecture Notes in Networks and Systems* (pp. 73–79). https://doi.org/10.1007/978-3-030-83175-2_11

Kang, J., & Rhee, H. (2025). Gender identity and perception in virtual spaces: the impact of avatar gender transition on the ZEPETO platform. *Frontiers in Virtual Reality*, *6*. https://doi.org/10.3389/frvir.2025.1505624

Kim, S., Youn, C., Cho, E., & Kim, S. (2025). When virtual influencers cause service failures: The impact of human likeness and beauty types on social psychological distance and consumer intentions. *Journal of Retailing and Consumer Services*, *87*, 104426. https://doi.org/10.1016/j.jretconser.2025.104426

Kuznetsova, O. A., Madzhumayev, M. M., & Grebenev, R. V. (2025). Metacrimes: Criminal Legal Assessment of Offences in AI-Driven Virtual and Augmented Realities (Metaverse). In *Lecture Notes in Networks and Systems* (pp. 120–128). https://doi.org/10.1007/978-3-031-97985-9_15

Larasati, Y. G., Fernando, H., Fitri, W., Wuysang, J. M., Hardianti, F., & Akbar, R. A. (2026). Young Children in War-Time: Making Sense of Palestine-Israel Conflict Impact on Instagram. *Italian Sociological Review*, *16*(1), 181–198. https://doi.org/https://doi.org/10.13136/isr.v16i1.977

Larasati, Y. G., Fernando, H., & Morin, L. (2025). The Stories of Death in Abangan. *Societas Dei: Jurnal Agama Dan Masyarakat*, *12*(1), 45–66. https://doi.org/10.33550/sd.v12i1.516

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Magableh, H. Y., & Al-Shawabkeh, B. K. A. (2024). The Problem of Jurisdictional Conflict and the Applicable Law on Cybercrime. *Pakistan Journal of Criminology*, *16*(3), 1287–1298. https://doi.org/10.62271/pjc.16.3.1287.1298

Martha, A. E. (2024). Perundungan Siber (Cyberbullying) Melalui Media Sosial Instagram dalam Teori the Space Transition of Cybercrimes. *Jurnal Hukum Ius Quia Iustum*, *31*(1), 199–218. https://doi.org/10.20885/iustum.vol31.iss1.art9

Melis, G., & Monaro, M. (2025). Sexual Crimes in Metaverse: New Frontiers in Forensic Psychology and Legal Challenges. *Journal of Metaverse*, *5*(2), 124–131. https://doi.org/10.57019/jmv.1658955

Narayanan, S., Polys, N., & Bukvic, I. I. (2020). Cinemacraft: exploring fidelity cues in collaborative virtual world interactions. *Virtual Reality*, *24*(1), 53–73. https://doi.org/10.1007/s10055-019-00382-0

Ojha, N. K., & Vaish, A. (2025). Legal and Ethical Issues in the Interaction of AI and Metaverse. In *Exploring AI Implications on Law, Governance, and Industry* (pp. 155–176). https://doi.org/10.4018/979-8-3373-3384-7.ch006

Pandey, P. (2025). Bits and Bytes Betrayal: Unravelling the Dark Threads of Cybercrime in the Metaverse. In *Security and Privacy in Smart Environments* (pp. 120–148). https://doi.org/10.1007/978-3-031-66708-4_6

Qin, H. X., Wang, Y., & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanities and Social Sciences Communications*, *12*(1), 194. https://doi.org/10.1057/s41599-024-04266-w

Roth, D., Bloch, C., Schmitt, J., Frischlich, L., Latoschik, M. E., & Bente, G. (2019). Perceived Authenticity, Empathy, and Pro-social Intentions evoked through Avatar-mediated Self-disclosures. *Proceedings of Mensch Und Computer 2019*, 21–30. https://doi.org/10.1145/3340764.3340797

Scott, B. (2023). Protecting Vulnerable Consumers Within the Metaverse. In *Influencer Marketing Applications Within the Metaverse* (pp. 117–131). https://doi.org/10.4018/978-1-6684-8898-0.ch008

Sepulveda, C. E. L., Taherdoost, H., & Farhaoui, Y. (2025). Balancing Data Protection in the Age of Digitization. In *Lecture Notes in Networks and Systems* (pp. 701–708). https://doi.org/10.1007/978-3-031-88304-0_95

Setiyawan, N. E., Karauwan, D. E. S., Jumiran, & Ghafar, A. A. (2024). The Effect of Digital Technology on Criminal Law Enforcement: an Analysis of Cybercrime and its Handling. *Mawaddah: Jurnal Hukum Keluarga Islam*, *2*(2), 229–248. https://doi.org/10.52496/mjhki.v2i2.169

Sharma, A., Kumar, S., Singh, S. K., Jawla, S., Arya, V., & Chui, K. T. (2025). Virtual Identity and Self-Expression in the Metaverse. In *Unveiling Social Dynamics and Community Interaction in the Metaverse* (pp. 93–110). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-8628-6.ch005

Sideris, L. H. (2011). I See You: Interspecies Empathy and Avatar. *Journal for the Study of Religion, Nature and Culture*, *4*(4), 457–477. https://doi.org/10.1558/jsrnc.v4i4.457

Tilley, N., & Sidebottom, A. (2014). Situational Crime Prevention. In *Encyclopedia of Criminology and Criminal Justice* (pp. 4864–4874). Springer New York. https://doi.org/10.1007/978-1-4614-5690-2_549

Tiwari, M., Zhou, Y., Gilmour, P., & Bernot, A. (2025). Confronting metacrime: complexities, enforcement challenges, and regulatory pathways. *Law, Innovation and Technology*, *17*(1), 159–176. https://doi.org/10.1080/17579961.2025.2469347

Tschanter, J., Merz, C., Wienrich, C., & Latoschik, M. E. (2026). How Harassment Shapes Self-Perception and Well-Being in Social VR: Evidence from a Controlled Lab Study. *IEEE Transactions on Visualization and Computer Graphics*, 1–11. https://doi.org/10.1109/TVCG.2026.3680575

Unesa. (2025). *Perang Siber dan Ancaman Keamanan Digital Global di Tahun 2025*. https://agridigi.fkp.unesa.ac.id/post/perang-siber-dan-ancaman-keamanan-digital-global-di-tahun-2025

Valera, L., Alamos, F., Ramos, P., & Vera, T. (2026). Bodies in the metaverse: Is there

"someone" out there? *AI & SOCIETY*, *41*(1), 99–110. https://doi.org/10.1007/s00146-025-02439-y

Webb, S. (2001). Avatarculture: Narrative, power and identity in virtual world environments. *Information, Communication & Society*, *4*(4), 560–594. https://doi.org/10.1080/13691180110097012

Wiwoho, J., Kharisma, D. B., & Wardhono, D. T. K. (2021). Financial Crime In Digital Payments. *Journal of Central Banking Law and Institutions*, *1*(1), 47–70. https://doi.org/10.21098/jcli.v1i1.7

XinYing, C., Tiberius, V., Alnoor, A., Camilleri, M., & Khaw, K. W. (2024). The Dark Side of Metaverse: A Multi-Perspective of Deviant Behaviors From PLS-SEM and fsQCA Findings. *International Journal of Human–Computer Interaction*, *41*(5), 3128–3148. https://doi.org/10.1080/10447318.2024.2331875

Yang, L., Xu, Y., & Hui, P. (2025). Framing metaverse identity: A multidimensional framework for governing digital selves. *Telecommunications Policy*, *49*(3), 102906. https://doi.org/10.1016/j.telpol.2025.102906

Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, *19*(3), 419–439. https://doi.org/10.1007/s11417-024-09436-y