Cybercrime Prosecution in the Metaverse: Evidentiary and Jurisdictional Challenges

1. Thabo Mokoena: Department of Public Law, University of Pretoria, Pretoria, South Africa
2. Eleni Papadopoulou*: Department of Political Science, University of Piraeus, Piraeus, Greece
3. Camila Rodríguez: Department of Law, Universidad de los Andes, Bogotá, Colombia

***Correspondence: e-mail: eleni.papadopoulou@unipi.gr

Abstract

The emergence of the metaverse as an immersive, persistent, and decentralized digital ecosystem introduces complex challenges for criminal law, evidence collection, and transnational enforcement. Unlike traditional cyberspace, the metaverse integrates virtual reality, artificial intelligence, and blockchain technologies to create embodied environments in which users interact through avatars, possess digital assets, and engage in real-time spatial behaviors. This multidimensional architecture redefines the nature of cyber-offending, enabling new forms of harm—including avatar-based assault, identity manipulation, NFT theft, biometric exploitation, and socially engineered deception—that do not easily conform to existing legal categories. This narrative review examines the evidentiary, jurisdictional, and regulatory difficulties that arise when prosecuting metaverse-based crimes. The analysis highlights the volatility and fragmentation of immersive digital evidence, which complicates scene reconstruction, behavioral interpretation, and authentication of avatar actions. Real-time spatial interactions, AI-assisted gesture generation, and decentralized data flows further challenge forensic reliability. Jurisdictional barriers intensify these issues, as offenders, victims, servers, and platform operators often reside in different regions, undermining traditional territorial principles and limiting the effectiveness of mutual legal assistance mechanisms. The review also evaluates the inadequacies of current national cybercrime frameworks, which rarely recognize metaverse-specific harms, and the shortcomings of international conventions that were developed for earlier forms of cybercrime. Gaps in definitions of virtual property, identity integrity, biometric protections, and smart-contract liability hinder consistent regulation. In addition, the dominance of private platform governance restricts access to critical evidence and weakens state enforcement capacity. The paper concludes that meaningful progress requires metaverse-aware legislative reforms, adaptive forensic methodologies, and enhanced international coordination. Without systematic modernization, legal systems will remain ill-equipped to address the evolving landscape of immersive digital crime.

Keywords: Metaverse; cybercrime; virtual evidence; jurisdiction; digital forensics; blockchain assets; avatar identity; decentralized platforms; international law; immersive environments

Received: date: 16 November 2022
Revised: date: 19 December 2022
Accepted: date: 31 December 2022
Published: date: 01 January 2023

Citation: Mokoena, T., Papadopoulou, E., & Rodríguez, C. (2023). Cybercrime Prosecution in the Metaverse: Evidentiary and Jurisdictional Challenges. *Legal Studies in Digital Age,* 2(1), 53-67.

1. Introduction

The emergence of the metaverse as a new socio-technical environment has introduced a paradigm shift in the way digital interactions, transactions, and social experiences unfold. Built on the convergence of immersive virtual reality (VR), augmented reality (AR), artificial intelligence, spatial computing, blockchain ecosystems, and persistent multi-user environments, the metaverse has rapidly evolved from a speculative concept to an operational digital layer that increasingly resembles an extension of lived reality. Its development is motivated by technological advancements that allow individuals to inhabit three-dimensional, embodied digital spaces through avatars that simulate presence, agency, and interaction in ways that fundamentally differ from traditional two-dimensional online platforms. As scholars have noted, the metaverse generates a reconstructed sense of personal identity and immersive embodiment that amplifies the psychological, expressive, and socio-behavioral elements of user engagement, making it qualitatively distinct from earlier forms of digital communication (Mitrushchenkova, 2023). This unprecedented layering of physical and digital experience stages a new frontier in human-computer interaction whose implications for criminality, evidence, and jurisdiction are only beginning to be understood.

The growing normalization of immersive virtual environments has been accompanied by a parallel increase in cyber-offenses that exploit the unique features of VR and AR systems. The shift toward embodiment, for example, has expanded the vulnerability of users to novel forms of identity theft where attackers infiltrate accounts not simply to access data but to manipulate avatar identities, behavioral patterns, or expressive features that blur the distinction between digital representation and personal autonomy. Psychological research highlights how virtual embodiment intensifies emotional resonance, opening the possibility for crimes that target users' emotional states, sense of agency, or perceived personal boundaries (González-Tapia, 2023). These offenses include virtual assault, stalking, harassment, or deception—forms of wrongdoing that occur within immersive spaces yet produce real psychological and legal harms. Image-based violence, which has long been documented in conventional digital platforms, has taken on new dimensions in VR environments, mirroring global concerns about technologically facilitated abuse (Sánchez, 2022). With full-body avatars, haptic interfaces, and motion-tracked interactions, perpetrators can engage in conduct that mimics physical intrusion or coercion, thereby raising questions about whether traditional legal categories adequately capture the type and severity of harm inflicted in immersive settings.

Financially motivated cyber-offenses have likewise multiplied as virtual economies mature. In many metaverse platforms, users purchase virtual land, digital merchandise, or tokenized assets that derive value from blockchain-based systems. This evolving digital economy has created opportunities for fraud, phishing, unauthorized transactions, and the theft of virtual property that is legally ambiguous yet financially significant. Criminal networks have begun exploiting these environments not only for economic gain but also for transactional cover, utilizing the anonymity, decentralization, and global accessibility of immersive platforms to mask illicit conduct. The complexity and scale of such activities have been documented in studies evaluating the strategies used by international cyber-offending groups, who increasingly rely on cross-platform coordination and sophisticated anonymity techniques to evade detection (Gundur et al., 2021). These developments underscore the growing intersection between immersive technology and cybercriminal innovation.

One of the most concerning evolutions has been the proliferation of deepfake impersonation and AI-generated behavioral manipulation within VR and AR settings. The metaverse's emphasis on real-time behavioral data—including voice, gesture, facial expression, movement patterns, and emotional cues—creates an unprecedented pool of biometric information that can be captured, replicated, or manipulated without users' awareness. Scholars have warned that the psychological realism of virtual interactions, coupled with the technical feasibility of recreating someone's avatar or voice with minimal data, heightens the risk of expressive and identity-based crimes (González-Tapia, 2023). Such offenses challenge existing conceptions of fraud, impersonation, coercion, or misrepresentation, especially when an avatar becomes a proxy for an individual's agency. This raises pressing evidentiary questions: what constitutes proof of identity in an environment where avatars can be cloned, modified, or puppeteered by third parties? How should courts evaluate digital traces that may—or may not—correspond to a user's real-world actions?

The combination of immersive embodiment, decentralized economies, and dynamic user-generated content creates a landscape where legal systems struggle to keep pace with emerging forms of criminality. Traditional legal frameworks were not designed for environments where a single user can simultaneously inhabit multiple digital spaces, interact through multiple avatars, and engage in transactions that traverse jurisdictions without leaving conventional trails. Scholars examining the socio-economic profiles of cybercrime victims have observed that disparities in digital literacy, technological infrastructure, and regulatory development shape the vulnerabilities of different populations in complex ways (Yarovenko et al., 2023). These structural disparities become even more pronounced in the metaverse, where access to secure devices, privacy-protective tools, and technical expertise significantly affects one's exposure to risk. This creates an uneven distribution of harm that spans borders, challenging states' ability to coordinate criminal justice responses.

As cyber-offenses escalate within immersive environments, legal systems face unprecedented challenges regarding evidence collection, authentication, and admissibility. Unlike traditional cybercrime investigations, which rely on data logs, metadata, device forensics, or IP-based tracking, metaverse investigations must reconstruct events occurring within three-dimensional virtual spaces. VR interactions are ephemeral, multi-layered, and often processed locally on users' devices rather than stored centrally. Even when platforms retain some form of analytics, telemetry, or behavioral data, such information is not standardized across systems and may not meet evidentiary standards in court. The complexity deepens when decentralized infrastructures—particularly those using blockchain—host transactions that are immutable but pseudonymous. Researchers have emphasized the importance of establishing secure chains of custody for digital evidence, highlighting the need for distributed verification frameworks that maintain evidentiary integrity in cross-platform environments (Alruwaili, 2021). However, existing chain-of-custody models may be ill-equipped to handle the dynamic and heterogeneous data streams generated within immersive spaces.

Complicating matters further, the metaverse's governance architecture is primarily driven by private platform operators rather than public legal authorities. Many immersive environments function as privately owned digital territories where platform administrators control data access, rule-enforcement mechanisms, user sanctions, and investigative cooperation. As a result, law enforcement agencies often rely on voluntary collaboration from private companies to secure evidence, identify offenders, or reconstruct virtual events. This resembles broader trends in cybercrime governance highlighted in earlier research, which notes that criminal justice actors increasingly depend on private intermediaries whose incentives may not align with public legal priorities (Brants et al., 2020). In the metaverse, where platforms may hold proprietary algorithms, encrypted interaction logs, or anonymized behavioral datasets, investigatory barriers can be even more pronounced. The absence of clear legal obligations governing evidence preservation, data transparency, or investigatory cooperation exacerbates these challenges, creating a patchwork of compliance practices that hinder efficient prosecution.

Jurisdictional ambiguity is arguably the most complex challenge associated with metaverse-related crimes. Immersive environments are inherently transnational: users interact across borders, servers are distributed globally, and transactions occur in decentralized ecosystems that defy territorial boundaries. Scholars exploring the legal conundrums of the metaverse emphasize that the concept of locus delicti—the place where a crime occurs—becomes difficult to define when wrongdoing unfolds within virtual spaces that are not anchored to physical geography (Kasiyanto & Kilinc, 2022). This problem is magnified when individuals engage in actions that simultaneously produce effects in multiple jurisdictions, such as NFT-based fraud, cross-border virtual asset transfers, or psychological harms inflicted on users located in different countries. Without clear territorial markers, states struggle to assert jurisdiction, initiate investigations, or coordinate prosecutions.

The international nature of metaverse governance also raises issues of sovereignty, regulatory fragmentation, and inter-jurisdictional conflict. While some countries prioritize user protection, privacy regulation, and transparency, others emphasize economic innovation, technological growth, or platform autonomy. Research analyzing the role of international institutions underscores the need for coordinated global governance mechanisms, noting that fragmented regulatory approaches hamper the creation of stable digital ecosystems (Abbasi, 2023). In the context of the metaverse, where platform operators may be headquartered in one jurisdiction, their servers hosted in another, and users distributed across dozens more, the absence of harmonized legal frameworks creates significant obstacles to prosecuting cyber-offenders. Efforts to establish international protocols for cross-border cybercrime investigations have long been complicated by concerns over privacy, sovereignty, and surveillance, challenges that are amplified within immersive contexts.

Moreover, the narrative dimensions of cybercrime—how it is conceptualized, interpreted, and communicated—may shape legal responses in significant ways. Earlier work examining cybercrime discourse has shown that public, legal, and institutional narratives about digital wrongdoing influence both legislative developments and enforcement priorities (Brants et al., 2020).

In the metaverse, the novelty of immersive offenses and the sensational nature of avatar-based harm risk generating either exaggerated fears or minimized interpretations. For example, crimes such as virtual assault may be dismissed as harmless digital interactions despite their documented emotional impact, while other offenses may be over-criminalized due to limited understanding of the technology. These narrative tensions complicate policymaking and hinder the development of balanced legal responses grounded in evidence rather than sentiment.

Given these complexities, existing legal frameworks remain insufficiently equipped to address the unique evidentiary and jurisdictional challenges of prosecuting cybercrime in the metaverse. Traditional doctrines of intent, consent, identity, and territoriality must be re-evaluated in a context where digital embodiment—and the technological systems that support it—mediate action. Immersive environments allow users to engage in behaviors that blur the line between intentional action and automated avatar responses, raising questions about culpability and agency. Likewise, the capacity for platform architects to manipulate or influence user behavior through algorithmic design introduces novel concerns regarding consent. These conceptual tensions illustrate the legal gap between established criminal doctrines and emerging technological realities.

Scholars examining digitally mediated identity have emphasized that users' self-representation in the metaverse operates at the intersection of psychological projection, technological architecture, and social interpretation (Mitrushchenkova, 2023). When identity itself becomes a composite of user input, platform algorithms, and system-generated behavior, evidentiary analysis becomes inherently complicated. Courts must determine whether observed avatar behavior corresponds to a user's intentional actions, accidental triggers, external manipulation, or system anomalies. The challenge extends to authentication: in environments where identity is fluid, customizable, and easily replicated, establishing the authorship or origin of virtual conduct requires sophisticated forensic methods that many jurisdictions have yet to develop.

The rapid pace of development has outstripped the capacity of legislators, courts, and investigative agencies to adapt. As a result, there exists a significant gap in coherent legal frameworks that can adequately address issues of evidence collection, admissibility, and cross-border prosecution within immersive virtual environments. Despite growing academic attention to the risks associated with virtual identity manipulation, emotional exploitation, image-based harm, and transactional cyber-offenses, there remains a lack of unified doctrinal guidance that integrates these concerns into a comprehensive regulatory strategy. Scholars across legal and socio-technical fields have repeatedly pointed out that emerging digital environments require specialized legal analysis, not merely the extension of traditional cybercrime laws into a new domain.

This narrative review therefore aims to synthesize existing research on the evidentiary and jurisdictional challenges associated with prosecuting cybercrime in the metaverse, using a descriptive analytical approach to evaluate the doctrinal, technological, and institutional barriers that impede effective legal governance. The objective of this review is to provide a comprehensive, multidisciplinary understanding of how immersive virtual environments transform the nature of digital criminality, and to identify the critical gaps that legal systems must address to ensure the fair and effective prosecution of metaverse-based offenses.

2. Conceptual Foundations

The conceptual foundations of the metaverse, along with the varieties of cybercrimes that occur within it and the legal status of its core components, form the basis for understanding the profound evidentiary and jurisdictional challenges that arise when prosecuting wrongdoing in immersive virtual environments. While public discourse often characterizes the metaverse as an extension of existing online platforms, legal scholarship, socio-technical research, and behavioral studies consistently demonstrate that this environment represents a qualitative transformation rather than a mere technological upgrade. The metaverse relies on deeply immersive architectures that blend persistent virtual spaces with sophisticated computational systems, altering not only the modes of human interaction but also the nature of criminal activity, identity formation, and digital property relations. These conceptual shifts underpin the legal complexities that emerge when traditional doctrines—developed for physical or two-dimensional digital contexts—are applied to three-dimensional, embodied, and decentralized environments.

The metaverse can be understood as a persistent, interconnected digital ecosystem composed of immersive environments where users interact through embodied avatars, conduct transactions, consume services, and engage in collaborative or social activities mediated by advanced computational technologies. Although many definitions exist, the most analytically useful perspectives conceptualize the metaverse as a socio-technical system in which virtual spaces are continuous, interoperable, and augmentable. Scholars examining virtual identity emphasize that the metaverse cannot be reduced to isolated VR applications; rather, it is a multilayered network of interconnected platforms whose architecture enables seamless transitions, digital presence, and the projection of selfhood into shared virtual spaces (Mitrushchenkova, 2023). This understanding highlights several defining characteristics, including interoperability, persistence, embodiment, and decentralization, all of which reshape how law must conceptualize action, harm, and evidence within immersive environments.

Interoperability refers to the metaverse's capacity to allow users, avatars, assets, and data to move across different virtual environments without friction. This feature distinguishes the metaverse from earlier virtual worlds or online platforms, which typically operated as closed ecosystems. The ideal of interoperability envisions a network of platforms that share protocols, identity systems, asset frameworks, and communication architectures. This vision presents technical and legal challenges because interoperability requires alignment across jurisdictions, standards, and proprietary systems. Scholars analyzing the governance implications of global digital ecosystems have emphasized that when platforms cross national, institutional, and regulatory boundaries, the risks associated with cybercrime, identity manipulation, and transactional fraud increase substantially (Abbasi, 2023). In immersive environments, these risks are amplified by the fact that interoperability may obscure the location, ownership, or provenance of digital interactions, complicating forensic reconstruction and jurisdictional assertions.

Persistence is another foundational attribute of the metaverse. Persistent virtual environments do not reset when users disconnect; rather, they continue to evolve, store state changes, and preserve the outcomes of interactions. Unlike conventional gaming environments, which may reset at the end of a session or operate in isolated instances, metaverse platforms maintain a continuous virtual world shared among users. This persistence has significant implications for digital evidence. If a virtual environment evolves organically even when a user exits, identifying the precise state of a scene at a specific moment becomes challenging. The persistence of virtual spaces also raises concerns about long-term data retention and traceability, issues that scholars studying emotional and representational harms in digital environments have highlighted as crucial to understanding the continuity between virtual actions and real-world psychological experiences (González-Tapia, 2023). Persistence thus introduces evidentiary tension: while continuous records may aid investigations, they also generate privacy risks, storage burdens, and verification complications if data are altered, deleted, or modified by platform operators.

Embodiment in the metaverse refers to the use of avatars—digital proxies that represent users in immersive environments. Embodiment can be partial, as in the use of head-and-hand tracking systems, or full, as in advanced motion capture interfaces that replicate facial expressions, gestures, and bodily movement. Scholars exploring the psychological dimensions of virtual identity argue that embodiment intensifies the sense of presence and emotional resonance, making interactions within immersive environments qualitatively comparable to real-life encounters (González-Tapia, 2023). This has profound implications for criminal law, especially when evaluating harms such as harassment, stalking, intimidation, or assault carried out through avatar-based actions. Embodiment creates evidentiary demands: investigators must determine whether the avatar's actions correspond to the user's intentional movements or whether they were automated, system-generated, or manipulated by third parties. This problem becomes more pronounced given research demonstrating that virtual identity is fluid, customizable, and susceptible to external influence (Mitrushchenkova, 2023). Questions of agency, authorship, and responsibility thus become central to legal analysis.

Decentralization further distinguishes the metaverse from earlier computational ecosystems. Many contemporary platforms integrate blockchain technology, decentralized storage, peer-to-peer networks, and smart contracts to manage digital identity, asset ownership, and transactional validity. Blockchain-based architectures allow virtual assets—such as NFTs, tokenized objects, or digital land parcels—to be stored, transferred, and authenticated without relying on a central authority. However, decentralization complicates legal intervention. Research on cross-border digital criminality emphasizes that the absence of central intermediaries significantly reduces the capacity of law enforcement to trace, seize, or freeze digital assets, particularly when they circulate across multiple blockchains or through mixers and privacy-enhancing tools (Gundur et al., 2021). Decentralization challenges traditional investigative techniques, chain-of-custody maintenance, and the extraction of logs or records that courts require to evaluate the authenticity of evidence.

Beyond these architectural attributes, the metaverse relies on a constellation of technologies whose interactions form the substrate of immersive digital environments. Virtual reality and augmented reality systems provide the sensory and spatial framework for user experiences. VR headsets, haptic gloves, eye-tracking systems, and full-body motion sensors render interactions as three-dimensional, embodied activities. AR overlays blend digital and physical environments, creating hybrid experiences. These systems collect vast quantities of biometric data—gesture profiles, movement signatures, gaze trajectories, voice patterns, emotional cues—creating both opportunities for forensic analysis and risks of privacy violations. Behavioral data recorded through immersive devices may help reconstruct the sequence of events during a cyber-offense, but they also expose users to exploitation if intercepted, manipulated, or stolen.

Artificial intelligence plays an equally critical role. AI algorithms govern avatar behavior, content moderation, system responsiveness, NPC interactions, environmental adaptation, and real-time translation. They influence social dynamics and may inadvertently shape user actions through reinforcement mechanisms. Scholars examining the socio-psychological implications of emotional expression in virtual environments note that AI-generated cues can amplify or mediate user behavior, making the boundary between autonomous action and system influence difficult to distinguish (González-Tapia, 2023). From a legal standpoint, this raises questions about whether harmful conduct should be attributed to users, platform algorithms, or a combination of both. It also complicates evidentiary evaluation when AI-generated elements form part of an interaction under investigation.

Blockchain technologies underpin digital asset systems within the metaverse. Virtual goods—avatars, skins, land, objects, collectibles—are often tokenized as NFTs or stored in decentralized ledgers. These structures allow users to demonstrate ownership, transfer assets, or engage in trade. Yet, legal scholars analyzing the regulatory complexity of the metaverse note that the tokenization of virtual assets introduces layers of ambiguity concerning property rights, contractual obligations, and jurisdictional authority (Kasiyanto & Kilinc, 2022). For instance, while blockchain records provide transparent transaction histories, pseudonymity obscures user identities. Additionally, smart contracts—self-executing code used to manage digital interactions—operate across jurisdictions without clear legal oversight. These features create opportunities for fraud, hacking, and theft, which present new challenges for prosecution.

Internet of Things (IoT) integration further contributes to the metaverse's infrastructure. IoT devices, sensors, and wearable technologies supply real-time data streams that synchronize physical and virtual experiences. Smart home systems, wearable biometric monitors, and connected devices may all feed information into immersive platforms, creating complex cross-domain interactions. Scholars studying cybercrime victimization emphasize that increased connectivity makes users more vulnerable to exploitation because IoT components often have weaker security protocols and generate sensitive data (Yarovenko et al., 2023). When IoT data synchronize with virtual environments, attackers may exploit these mechanisms to conduct cross-platform attacks or extract personal information that influences user behavior within immersive contexts.

Digital asset systems represent another core layer of metaverse architecture. These systems include virtual currencies, blockchain assets, tokenized objects, platform-specific credits, and hybrid payment mechanisms. Virtual economies often operate on decentralized exchanges or marketplace platforms where the boundaries between real money and digital assets blur. Scholars have documented how criminal networks exploit these systems for cross-border transfers, laundering, or fraud, taking advantage of decentralized architectures to obscure illicit behavior (Gundur et al., 2021). The interdependence of blockchain systems, platform infrastructures, and user interactions creates a complex web that investigators must navigate when pursuing metaverse-related crimes.

Altogether, the metaverse's technical architecture introduces multidimensional challenges for legal governance, evidentiary evaluation, and jurisdictional authority. Its reliance on persistent environments, interoperable networks, decentralized infrastructures, and AI-mediated interactions fundamentally alters the nature of digital behavior. As scholars highlight, the metaverse reshapes identity, social engagement, and emotional expression in ways that demand new legal frameworks and interpretive models (Mitrushchenkova, 2023). Understanding these foundations is crucial for analyzing the typology of cybercrimes that emerge within immersive virtual environments.

The metaverse's architectural complexity gives rise to unique forms of cyber-offenses that differ substantially from traditional online crimes. These offenses exploit immersive embodiment, real-time interactions, biometric data streams, decentralized economies, and avatar-based presence. While some behaviors reflect familiar cybercrimes such as fraud, harassment, or identity theft, the means by which they occur—and the harm they produce—are shaped by the distinctive characteristics of three-dimensional environments. Scholars analyzing sexualized digital violence, identity manipulation, and emotionally mediated harms emphasize that immersive contexts magnify the psychological impact of wrongdoing and blur the distinction between virtual and real-world victimization (González-Tapia, 2023; Sánchez, 2022). As a result, metaverse cybercrimes require new doctrinal interpretations and analytical categories.

One foundational category is cyber-trespass, which involves unauthorized access to virtual spaces or accounts. In immersive environments, trespass may occur when an offender infiltrates another user's virtual property, manipulates system permissions, or bypasses platform controls to observe or interact within restricted areas. Unlike traditional hacking, cyber-trespass in the metaverse may include spatial violations that mimic physical intrusion. For example, an attacker who enters a user's virtual home uninvited may provoke psychological fear, disruption, or emotional distress, even though the intrusion occurs in a digital environment. Scholars examining the socio-psychological effects of virtual interactions note that spatial boundaries in immersive contexts are experienced similarly to physical boundaries, making cyber-trespass an emotionally salient offense (González-Tapia, 2023). This raises questions about whether traditional trespass laws—designed for physical property—adequately address harm within virtual spaces.

Avatar-based harms represent another significant category. These offenses include harassment, stalking, intimidation, assault-like interactions, or coercion carried out through avatar actions. Since avatars serve as embodied proxies, harmful conduct directed at an avatar may be experienced as directed at the user personally. Researchers studying personal identity in the metaverse highlight that avatars reflect an intricate combination of self-representation, emotional investment, and social recognition (Mitrushchenkova, 2023). When an avatar is assaulted, touched without consent, or subjected to harassment, the user may experience real psychological harm. Because virtual assault may involve mimicry of physical actions, including grabbing, hitting, or groping, victims often report intense emotional reactions that challenge the conventional legal view of cyber-harm as primarily informational rather than embodied. These harms also produce evidentiary complications, as avatar interactions may not be recorded, may be manipulated by platforms, or may not clearly reflect user intent.

Biometric data theft constitutes a third major category of metaverse cybercrime. Immersive devices collect facial expressions, eye movements, heartbeat data, voice signatures, gesture dynamics, motion profiles, and emotional-response indicators. These data streams create highly sensitive personal profiles that attackers can exploit to impersonate users, manipulate behavior, or craft targeted attacks. Scholars have emphasized that biometric theft within immersive environments is particularly harmful because it enables avatars to be replicated convincingly, leading to deepfake impersonation or behavioral cloning (González-Tapia, 2023). The theft of gaze-tracking data, for example, may reveal users' interests, fears, or behavioral tendencies, allowing attackers to perform intrusive psychological manipulation. Similarly, motion-capture profiles may be used to mimic a user's avatar movements, creating false evidence or facilitating identity fraud. These offenses challenge traditional cybersecurity frameworks, which often focus on traditional forms of personally identifiable information rather than real-time biometric signatures.

Virtual property crimes form another expanding category. These include NFT theft, virtual land fraud, unauthorized asset transfers, and the manipulation of digital marketplaces. The metaverse's reliance on tokenized assets creates unique opportunities for financial exploitation. Research examining the legal ambiguities of tokenized property highlights the lack of clarity surrounding ownership rights, contractual obligations, and liability structures (Kasiyanto & Kilinc, 2022). Attackers may steal NFTs representing virtual clothing, vehicles, weapons, or land parcels, sometimes worth substantial real-world value. Fraud may occur through rug-pull schemes, deceptive promotions, or market manipulation practices. Decentralized platforms provide criminals with tools to transfer assets across borders rapidly and anonymously, complicating both detection and prosecution. Traditional property laws struggle to classify these assets: are they commodities, intellectual property, securities, or contractual rights? The lack of consensus affects how courts handle disputes or evaluate criminal liability.

Social engineering in immersive spaces represents an increasingly dangerous form of cybercrime. Attackers exploit embodied interactions, emotional cues, and real-time engagement to deceive users. Research on cybercriminal transactional methods indicates that immersive environments create new opportunities for attackers to build trust, manipulate perception, or impersonate authoritative figures (Gundur et al., 2021). For example, an attacker may appear as a platform administrator, law enforcement officer, or fellow community member to extract personal information or coerce compliance. The realism of avatar interactions increases the effectiveness of social engineering because users respond to embodied cues—voice tone, facial expression, gesture patterns—in ways that mimic real-life social behavior. This makes them more susceptible to manipulation. Additionally, the use of deepfake avatars allows attackers to impersonate known individuals, facilitating emotional manipulation or financial scams. These techniques amplify harm and create evidentiary challenges: investigators must determine whether the manipulative avatar corresponds to a real user, an AI-generated agent, or a hybrid system controlled by multiple actors.

Image-based and video-based offenses also escalate in immersive environments. Scholars analyzing technologically facilitated sexual abuse emphasize that immersive platforms provide attackers with tools to create realistic simulations of victims or to capture sensitive interactions for exploitation (Sánchez, 2022). Offenders may record virtual encounters, manipulate avatar bodies, or create deepfake sexualized content using stolen biometric or visual data. These crimes blur the boundaries between virtual representation and real-world harm, raising complex legal questions regarding consent, exploitation, and the definition of sexual violence within digital spaces. Since virtual environments may lack structural safeguards or moderation tools, victims often experience repeated exposure to abusive content, compounding psychological harm.

Crimes involving collective or coordinated digital wrongdoing also emerge in the metaverse. Attackers may collaborate across platforms to conduct raids on virtual communities, disrupt social events, vandalize virtual property, or conduct targeted harassment campaigns. Research examining cybercrime victimization across countries suggests that groups with access to advanced technological tools—such as bots, behavioral scripts, or automated avatar systems—can inflict large-scale harm, disproportionally affecting vulnerable populations (Yarovenko et al., 2023). These coordinated offenses challenge law enforcement because they occur in decentralized, anonymous networks where attackers may distribute tasks across jurisdictions to evade detection.

Crimes targeting platform infrastructure constitute another category. Attackers may exploit vulnerabilities in the system architecture to manipulate system physics, override interaction rules, or disrupt environmental stability. These attacks may disable user protections, alter environmental states, or distort spatial dynamics. Because immersive interactions depend on complex synchronization across devices, servers, and user interfaces, such attacks may destabilize entire communities or create cascading failures that compromise evidence collection.

Altogether, the typology of metaverse cybercrimes illustrates the evolving nature of digital wrongdoing in immersive environments. These offenses challenge traditional legal categories and demand new frameworks for understanding how embodiment, decentralization, and real-time interactions shape criminal behavior. Existing scholarship across psychology, criminology, and law emphasizes that metaverse crimes must be interpreted through the lens of both technological architecture and user experience to develop appropriate legal responses (González-Tapia, 2023; Gundur et al., 2021; Sánchez, 2022).

The transformation of digital environments into immersive, embodied spaces demands a thorough re-evaluation of legal doctrines concerning identity, representation, property, and harm. Avatars, digital property, and virtual identity—core components of the metaverse—raise complex questions about personhood, agency, ownership, and the legal recognition of harm. Existing legal frameworks were developed for physical actors, tangible property, and informational records. These frameworks struggle to accommodate a landscape where users' identities are projected into embodied representations, where property exists as tokenized objects on decentralized ledgers, and where harm may occur through symbolic but emotionally salient interactions.

3. Evidentiary Challenges in Metaverse-Based Crimes

The rise of the metaverse as a multidimensional, immersive digital environment has radically altered the landscape of cybercrime investigation and prosecution. Traditional forensic models—developed for two-dimensional platforms, static records, and conventional digital traces—are ill-equipped to manage the complexity of evidence produced in three-dimensional, real-time virtual spaces. As users engage through embodied avatars and as interactions unfold dynamically across decentralized networks and private platforms, the challenges associated with collecting, authenticating, and presenting digital evidence intensify. At the conceptual level, the metaverse disrupts core assumptions embedded in criminal procedure, namely the stability of digital traces, the determinability of actions, the singularity of identity, and the reliability of system-generated records. Scholars studying cybercrime victimization have emphasized that the more complex and immersive the digital environment becomes, the more difficult it becomes to construct stable, verifiable narratives of wrongdoing (Yarovenko et al., 2023). These difficulties are magnified when immersive interactions depend on real-time rendering, AI mediation, biometric data-collection, and decentralized systems that lack uniform forensic standards.

The first major evidentiary challenge in metaverse-based crimes relates to the volatility of spatial data and the difficulties associated with capturing ephemeral interactions. Unlike traditional digital records—such as text messages, emails, or static screenshots—interactions within immersive environments unfold through spatialized, embodied, and temporally fluid exchanges. Virtual architectures simulate physical presence through visual, auditory, and haptic cues, and these environments evolve continuously even when individual users disconnect. Scholars examining emotional and avatar-based harm emphasize that immersive interactions rely on synchronized motion-tracking, gaze detection, voice input, and environmental physics, creating multi-layered data streams that are difficult to preserve in stable form (González-Tapia, 2023).

Because virtual environments prioritize performance and responsiveness, many systems avoid storing the full depth of interaction data. Instead, they process inputs locally, discard intermediate renderings, and store only partial logs. This design approach is intended to preserve user privacy and reduce system load, yet it significantly complicates forensic investigations. When a crime occurs—such as an avatar-based assault, stalking, or unauthorized intrusion—investigators must reconstruct a three-dimensional sequence of events that may not exist in persistent form. Scholars analyzing technologically facilitated abuse highlight that the challenge of reconstructing virtual interactions mirrors the difficulty courts traditionally faced with transient physical encounters, but amplified by the fact that the digital traces of immersive conduct often vanish quickly (Sánchez, 2022). Without synchronized motion data, gesture logs, and spatial coordinates, investigators may lack the raw material needed to determine what happened, who acted, and how intent manifested within the scene.

Reconstructing three-dimensional interactions is further complicated by the variability of metaverse platforms. Different systems adopt different rendering engines, interaction protocols, avatar frameworks, and logging conventions. Some platforms store full kinematic data, while others store only simplified interaction markers. Scholars studying metaverse identity caution that the architecture of each environment influences how identity, agency, and behavior are represented and therefore how they can be interpreted in legal settings (Mitrushchenkova, 2023). For example, a gesture detected as a harmful action in one system may be a default idle animation in another. If a platform uses AI-generated inference to fill gaps in motion-tracking—such as predicting the position of a limb when motion-capture data drops—this interpolation may distort the accuracy of evidence. Courts must therefore grapple with the fact that immersive evidence is not only volatile but also technologically mediated in ways that blur the line between user-generated and system-generated behavior.

Capturing haptic, voice, biometric, and behavioral cues introduces further complexity. Many immersive devices collect highly sensitive biometric data, including heartbeat patterns, eye movements, emotional responses, gait signatures, and facial expressions. These data streams are essential for the functionality of avatar systems, but they are rarely stored in raw form due to privacy concerns and technical constraints. Scholars analyzing distributed biometric systems highlight that the theft or misuse of such data poses severe risks for identity manipulation and impersonation (González-Tapia, 2023). Yet even when the data are not stolen, their absence as records complicates forensic reconstruction. If an offender uses a haptic glove to simulate unwanted physical contact with another user's avatar, for example, the specific force vectors, pressure points, and motion details may not be preserved. Similarly, voice interactions in immersive chat may be transmitted via spatialized audio systems that do not retain permanent logs. This mirrors broader issues in cybercrime investigations where ephemeral communication tools hinder evidentiary preservation, yet the complexity of VR interfaces amplifies these problems.

Behavioral cues—such as avatar proximity, movement style, interaction frequency, and gesture patterns—may be central to establishing intent or coercive behavior. Scholars examining international cyber-offending emphasize that behavioral analysis is often a critical component in reconstructing criminal methods, especially when offenders obscure their identity or use multiple platforms (Gundur et al., 2021). In the metaverse, behavioral cues may reveal whether an avatar approached another in a threatening manner, whether a user engaged in repeated stalking movements, or whether manipulative gestures were used during a social-engineering attack. However, because behavioral cues depend on real-time motion data that may not be preserved, investigators often rely on incomplete or inconsistent records.

The volatility of spatial data also affects scene integrity. In physical crime scenes, the environment typically remains static until investigators arrive. In digital environments, especially immersive ones, the scene continues to evolve even after the crime has occurred. Objects may be moved, avatars may return, environmental variables may shift, physics engines may adjust, and system updates may alter spatial configurations. Scholars analyzing the governance of metaverse infrastructure argue that these dynamic transformations undermine the stability of evidence and complicate efforts to establish a coherent narrative of events

(Abbasi, 2023). If a platform updates textures, reorganizes virtual architecture, or modifies interaction mechanics, the scene may no longer resemble the environment where the offense occurred.

Additional complexity arises from decentralized architectures. When interactions occur across distributed servers or peer-to-peer networks, logs may be fragmented across jurisdictions, stored in encrypted forms, or temporarily cached on user devices. Scholars examining blockchain systems argue that decentralization expands opportunities for anonymity and data fragmentation, making it difficult for investigators to obtain holistic records (Kasiyanto & Kilinc, 2022). When crimes involve digital asset transfers, investigators must trace transactions through blockchain networks that may include privacy layers, mixers, or complex multi-signature arrangements. These record types differ significantly from platform-generated logs, creating a hybrid evidentiary environment that requires multidisciplinary forensic expertise.

Ultimately, collecting evidence in immersive and real-time environments requires new investigative strategies. While traditional cyber-forensics focuses on extracting metadata, device logs, and static datasets, metaverse forensics must reconstruct spatialized interactions, verify biometric contributions, and interpret avatar-based behavior. Scholars studying the interplay between emotional states and virtual interactions emphasize that immersive experiences generate psychologically significant events whose legal interpretation depends on accurate reconstruction (González-Tapia, 2023). Without reliable evidence, courts may struggle to evaluate claims of harm, intent, or responsibility. This underscores the need for new evidentiary frameworks tailored to immersive digital environments.

Even when investigators successfully collect immersive digital evidence, challenges related to authenticity and integrity remain substantial. Immersive environments generate records that are vulnerable to manipulation, distortion, or misrepresentation, especially when AI-generated elements, avatar customization systems, and decentralized data structures shape user interactions. Ensuring the authenticity of metaverse evidence requires courts to evaluate not only the origin and accuracy of data but also the technological processes that produced them.

One major authenticity challenge arises from deepfake technologies. Scholars studying identity manipulation emphasize that the proliferation of deepfake tools, combined with the rich biometric inputs collected by immersive devices, allows attackers to produce highly realistic impersonations of users (González-Tapia, 2023). In the metaverse, deepfakes are not limited to video content; they can be applied to avatars, voice channels, gesture profiles, and behavioral signatures. Attackers may create an avatar that replicates a user's appearance, movement style, or vocal patterns to commit offenses. Investigators must therefore determine whether an avatar behavior captured in the logs corresponds to the real user or to an impersonating attacker. This problem mirrors concerns raised in studies of image-based abuse, where attackers manipulate digital representations of victims to cause harm (Sánchez, 2022). In immersive spaces, however, the complexity of behavioral data makes these determinations even more challenging.

Avatar spoofing poses similar risks. Attackers may hack an account, hijack an avatar, or clone its appearance. Research on metaverse identity highlights that avatars are central to users' sense of agency and embodiment, making their manipulation particularly harmful (Mitrushchenkova, 2023). When an attacker spoofs an avatar, they can perform actions that appear attributable to the victim, creating false evidence or framing them for wrongdoing. Investigators must therefore distinguish between actions performed by legitimate users and those performed by imposters. This requires robust authentication mechanisms, yet many immersive platforms rely on weak identity-verification systems, such as username-password combinations or easily stolen tokens.

AI-generated environments introduce another layer of complexity. Many immersive platforms use AI to generate dynamic environments, fill gaps in rendering, or simulate crowds. Scholars studying cybercrime narratives emphasize that system-generated content often blends seamlessly with user-generated content, complicating efforts to determine who—or what—initiated a particular event (Brants et al., 2020). AI-controlled avatars, AI-populated environments, or algorithmically generated behaviors may serve as evidence, yet their reliability depends on the accuracy of the underlying algorithms. If an AI system misinterprets input or generates unpredictable outcomes, courts must determine whether system artifacts can constitute reliable evidence.

Ensuring the integrity of digital evidence also requires addressing chain-of-custody challenges. Traditional digital-evidence frameworks rely on centralized storage, controlled access, and verifiable tamper-proof mechanisms. In decentralized metaverse platforms, however, records may be distributed across private servers, user devices, blockchain networks, and ephemeral cloud caches. Scholars analyzing distributed chain-of-custody systems argue that decentralized environments complicate efforts to ensure that evidence remains intact throughout its lifecycle (Alruwaili, 2021). If evidence is distributed across multiple nodes or reliant on platform-controlled logs, investigators must demonstrate that the data were not altered during transfer, storage, or retrieval. This is particularly difficult when platforms lack standardized forensic protocols or when private operators control access to core system logs.

Blockchain records present both opportunities and challenges for authenticity. Because blockchain transactions are immutable, courts may view them as reliable indicators of asset transfers or digital property ownership. However, pseudonymity makes it difficult to link blockchain entries to specific individuals, and attackers may use advanced obfuscation techniques to disguise their identity. Scholars examining criminal transactional methods highlight that blockchain-based anonymity tools, such as mixers or privacy coins, hinder investigative attribution (Gundur et al., 2021). When blockchain records are combined with in-platform logs, courts must determine how to reconcile decentralized and centralized evidence sources. Differences in timestamp protocols, timezone formats, consensus mechanisms, and data-recording methods introduce inconsistencies that undermine evidentiary coherence.

Integrity concerns also arise when platform operators have unilateral control over system logs. Private metaverse providers may modify, delete, or anonymize records as part of routine maintenance or privacy policies. Scholars analyzing international digital governance frameworks warn that when private companies hold exclusive control of essential records, they may inadvertently or intentionally alter potential evidence (Abbasi, 2023). Courts must therefore evaluate whether platform-generated logs are trustworthy, whether operators followed consistent policies, and whether commercial incentives influenced record handling.

The interoperability of immersive platforms further complicates authenticity. When users move assets or avatars across interconnected environments, evidence may traverse multiple systems. Each system may use different timestamp formats, resolution standards, logging conventions, and data-retention policies. As a result, the authenticity of evidence may depend on aligning heterogeneous records across incompatible systems. Scholars examining legal conundrums in the metaverse argue that interoperability undermines stable evidentiary chains because each platform contributes different layers of representation and interpretation (Kasiyanto & Kilinc, 2022). This creates a patchwork evidentiary landscape where investigators must integrate disparate data sources to reconstruct events.

Ultimately, authenticity and integrity concerns highlight the need for specialized evidentiary frameworks tailored to immersive environments. Courts must learn to evaluate behavioral data, motion-capture logs, biometric signatures, and blockchain transactions in ways that reflect the unique properties of the metaverse. Without reliable authenticity standards, prosecutors may struggle to attribute conduct, establish responsibility, or overcome challenges posed by deepfake technologies and decentralized platforms.

Once evidence is collected and authenticated, courts must determine whether it is admissible under procedural rules. The admissibility of metaverse-based evidence presents profound challenges because traditional evidentiary doctrines were developed for physical evidence or two-dimensional digital data. Immersive environments produce novel evidence types—three-dimensional reconstructions, avatar interactions, behavioral analytics, blockchain transactions, AI-generated artifacts—that do not fit neatly within existing legal categories. Scholars examining criminal justice responses to cybercrime emphasize that traditional courts often struggle to apply established rules to emerging technologies, especially when the underlying systems lack transparency or standardization (Brants et al., 2020).

One major admissibility issue concerns the standards for evidence derived from immersive platforms. Courts typically require that digital evidence be relevant, reliable, and not unduly prejudicial. However, determining relevance and reliability in immersive contexts is difficult. For example, a three-dimensional reconstruction of a virtual scene may appear highly persuasive to a jury, yet the reconstruction may be based on incomplete or interpolated data. Scholars examining emotionally mediated virtual interactions emphasize that immersive visualizations can evoke powerful reactions that may mislead fact-finders (González-Tapia, 2023). Courts must therefore decide whether immersive reconstructions constitute demonstrative evidence or substantive evidence, and whether their persuasive power outweighs potential risks of distortion.

Reliability concerns extend to VR logs, blockchain records, and platform-generated datasets. VR logs may contain gaps due to connectivity issues, sensor failure, or privacy controls. Scholars studying digital identity caution that gaps in motion-capture data may obscure critical behavioral cues needed to assess intent or harm (Mitrushchenkova, 2023). Blockchain records, while immutable, present timestamp discrepancies and pseudonymity barriers that reduce their evidentiary clarity. Platform-generated datasets—such as telemetry records, analytics, or interaction logs—may be proprietary, selectively retained, or influenced by system algorithms. Scholars examining governance mechanisms argue that private control of evidence raises concerns about selective disclosure, incomplete records, or conflicts of interest (Abbasi, 2023). Courts must therefore evaluate how much weight to assign to platform-generated evidence and whether its provenance can be independently verified.

Another admissibility challenge concerns the influence of privately owned platform governance. Metaverse environments are controlled by corporations that maintain their own rules, moderation practices, logging policies, and data-retention frameworks. Scholars examining international cybercrime enforcement note that dependence on private platforms undermines public accountability and creates inconsistencies in evidence availability (Gundur et al., 2021). When platforms reserve the right to alter records, suspend accounts, or delete logs, courts must determine whether the resulting evidence meets procedural standards. Additionally, platforms may lack incentive to preserve evidence, especially if doing so exposes them to liability or increases operational costs.

Jurisdictional diversity also affects admissibility. Different legal systems impose different standards for digital evidence. Some jurisdictions require stringent metadata documentation, while others apply flexible relevance-based tests. When metaverse crimes involve users, platforms, or servers located in multiple countries, courts may need to integrate evidence derived from systems with incompatible forensic standards. Scholars analyzing cross-border governance emphasize that legal fragmentation undermines the ability of courts to rely on foreign-collected evidence (Kasiyanto & Kilinc, 2022). If platform operators follow data-retention practices governed by foreign law, domestic courts may lack assurance that the evidence meets local admissibility standards.

In addition, courts must confront the challenge of AI-generated artifacts. AI systems produce logs, inference data, and predictive outputs that contribute to immersive interactions. Scholars examining technologically mediated criminality highlight that AI influence raises questions about authorship, agency, and evidentiary clarity (Brants et al., 2020). If evidence contains AI-inferred data, courts must determine whether such data meet the scientific reliability standards typically applied to expert evidence. They must also decide how to instruct juries about AI-mediated content to minimize bias or misunderstanding.

Ultimately, the admissibility challenges surrounding metaverse evidence reflect the broader transformation of digital environments. As immersive platforms become more prevalent, courts must develop new standards for evaluating the reliability of motion-capture data, three-dimensional reconstructions, blockchain records, biometric signatures, and platform-generated logs. Without clear admissibility frameworks, the prosecution of metaverse-based crimes will remain inconsistent and legally uncertain.

4. Jurisdictional and Territorial Challenges

The metaverse introduces unprecedented jurisdictional and territorial challenges that fundamentally reshape how states define, enforce, and coordinate legal authority. Traditional notions of territoriality and sovereignty developed in an era when crime, communication, and identity were primarily grounded in physical geography. The rise of the internet weakened but did not eliminate the link between criminal conduct and physical territory, since digital activities still depended on identifiable hardware, IP addresses, national service providers, and geographically anchored infrastructure. In contrast, the metaverse—composed of immersive, persistent, and interoperable environments built on decentralized systems—dissolves many of the spatial and institutional markers that states rely on to determine jurisdiction. Scholars studying cross-border cybercrime emphasize that as digital environments grow more complex and globally interconnected, states face increased difficulty identifying where cyber-offending occurs, where offenders are located, and which jurisdictions hold legitimate authority to prosecute wrongdoing (Gundur et al., 2021). These challenges intensify when offenses unfold within virtual spaces that lack geographic coordinates, are governed by private actors, and operate across blockchain networks and distributed servers.

The borderless nature of the metaverse represents one of the most profound jurisdictional challenges for criminal law. Unlike physical spaces, where territorial boundaries are fixed, observable, and enforceable, immersive environments operate independently of national geography. Users from multiple jurisdictions interact simultaneously in shared spaces, and their avatars occupy the same virtual environment regardless of where their physical bodies or devices are located. Scholars analyzing socio-economic patterns of cybercrime victimization emphasize that the globalization of digital environments exposes users from diverse regions to shared risks, creating a transnational victim landscape that challenges state-centered enforcement models (Yarovenko et al., 2023). Within the metaverse, this transnational exposure is amplified by real-time embodiment and decentralized networks.

The dissolution of traditional geographic boundaries makes it difficult to determine where a crime "occurs." In physical jurisdictions, locus delicti—the place where an offense takes place—is essential for asserting authority. Courts rely on territorial markers to determine applicable law, identify competent authorities, and establish connections between conduct and state interests. In virtual environments, however, conduct does not take place in physical space but through digitally mediated interactions rendered through servers, user devices, and platform architectures. Scholars examining metaverse governance frameworks note that virtual interactions are produced by rendering engines, AI algorithms, and distributed systems that process inputs across multiple jurisdictions (Abbasi, 2023). Thus, the location of an avatar's harmful act may correspond to no single physical geography; servers hosting the environment may reside in multiple countries; the perpetrator and the victim may be physically located in distant states; and platform operators may be headquartered elsewhere entirely.

This diffusion of spatial anchors complicates the definition of locus delicti. For example, if an avatar commits a virtual assault against another avatar within a metaverse space, determining the "location" of the crime may involve identifying the physical location of the perpetrator, the victim, the server hosting the environment, the company owning the platform, or the blockchain network that stores the interaction. Each of these loci corresponds to different jurisdictions, potentially generating overlapping, conflicting, or inconsistent claims of authority. Scholars studying identity and representation in immersive environments emphasize that avatars act as extensions of users' psychological and emotional presence, meaning that harmful conduct can have profound real-world effects despite lacking geographical anchoring (González-Tapia, 2023). This complicates jurisdictional reasoning because courts must decide whether virtual harms that produce real psychological or financial effects should be considered local, transnational, or extraterritorial.

Problems defining locus delicti become even more pronounced when offenses involve decentralized ecosystems. Blockchain-based interactions, such as NFT theft, asset manipulation, or fraud, may occur through smart contracts executed across nodes located globally. Scholars analyzing the legal structure of decentralized metaverse environments highlight that these systems undermine territoriality because they operate simultaneously across jurisdictions, and no single state can claim sovereignty over their infrastructure (Kasiyanto & Kilinc, 2022). Even when jurisdictions attempt to assert authority over blockchain interactions, they may face technical barriers to enforcement, particularly if nodes are distributed across countries with divergent legal frameworks.

The borderless nature of immersive worlds also affects investigative jurisdiction. When a crime occurs, law enforcement agencies typically request data from service providers within their jurisdiction. In the metaverse, critical evidence may be held by companies headquartered abroad, stored on servers in multiple countries, or distributed across blockchain networks that do not respond to government requests. Scholars examining international cybercrime enforcement note that the decentralization of data storage undermines traditional territorial enforcement models and forces states to rely on voluntary cooperation from private actors or cross-border agreements that may be slow and ineffective (Gundur et al., 2021).

Furthermore, global platform interoperability exacerbates jurisdictional fragmentation. Immersive environments increasingly allow users to transfer assets, identities, and avatars across multiple platforms. When digital identity and property move across systems, offenses may span several distinct virtual environments governed by different terms of service, logging practices, and technical architectures. Scholars analyzing the governance challenges of metaverse ecosystems emphasize that interoperability weakens jurisdictional clarity because interactions occur on layers that transcend any single regulatory framework (Abbasi, 2023). As a result, determining which environment's rules apply at a given moment becomes a significant challenge.

The borderlessness of the metaverse thus produces jurisdictional ambiguity at multiple levels: the location of the offense, the location of the parties, the location of the underlying infrastructure, and the governing framework for interactions. These complexities illustrate why traditional territorial principles struggle to apply to immersive environments and why states must reconsider how jurisdiction is conceptualized in a digital world that increasingly lacks geographical anchors.

Metaverse environments are not operated by governments but by private companies, decentralized networks, and transnational coalitions of developers, platform owners, and server hosts. This multi-stakeholder governance structure challenges traditional legal assumptions concerning state control, accountability, and enforcement. Scholars analyzing metaverse regulation emphasize that governance power is fragmented among platform operators, states, private server owners, blockchain communities, and third-party service providers (Abbasi, 2023). Each of these actors exercises influence over different components of the metaverse, creating overlapping and sometimes competing sources of authority.

Platform operators play a central governance role. They design the rules of interaction, moderate behavior, enforce community guidelines, and manage user data. Such rules often serve as de facto law within the virtual environment, governing user conduct regardless of national legal frameworks. Scholars examining cybercrime narratives highlight that private operators effectively become regulators of digital behavior, even though their incentives reflect commercial interests rather than public safety priorities (Brants et al., 2020). This produces tension between the responsibilities of states to enforce criminal law and the autonomy of platforms to manage their communities. Operators may choose to limit data retention to protect user privacy, reduce operational costs, or manage reputational risk, even when such decisions undermine law-enforcement efforts.

States, by contrast, assert authority through national cybercrime laws, but their reach is constrained by territorial limitations. Scholars studying cross-border digital infringement emphasize that state authority must contend with the fact that digital infrastructure often lies outside national borders (Yarovenko et al., 2023). When platform operators are headquartered abroad, or when virtual interactions occur through decentralized networks, states may find their enforcement capacity limited. States may demand data access, enforce subpoenas, or seek compliance with domestic regulations, but platform operators may resist on grounds of jurisdictional conflict, corporate policy, or user privacy protections.

Private server owners represent another layer of governance complexity. Some metaverse environments allow individuals or organizations to host private servers that simulate self-contained virtual worlds. These servers may operate under distinct rules that differ from those imposed by the platform operator. Scholars analyzing decentralized governance structures note that server owners effectively exercise territorial control over their virtual domains, determining what behaviors are permitted and how data are managed (Kasiyanto & Kilinc, 2022). Such autonomy complicates jurisdictional analysis: if a crime occurs on a privately hosted server located in a foreign country, identifying the responsible regulatory authority becomes difficult. Additionally, private server owners may not maintain adequate logs or implement forensic-ready architectures, complicating investigations.

Conflicts between national cybercrime laws and global platforms arise frequently. One jurisdiction may criminalize certain behaviors—such as avatar-based harassment, deepfake distribution, or virtual property theft—while another may not recognize these offenses. Scholars studying image-based abuse emphasize that national legal frameworks differ widely in how they define digital harm, consent, and exploitation (Sánchez, 2022). These divergences create conflict when offenders and victims reside in different jurisdictions with incompatible definitions of wrongdoing. For example, a user in one country may engage in avatar-based behavior that constitutes criminal harassment under local law, but the platform operator may be headquartered in a jurisdiction that does not recognize such conduct as actionable. This misalignment hinders enforcement and complicates cooperation.

Platform governance also affects the evidentiary landscape. Operators may have their own moderation logs, interaction data, and enforcement histories, but these are not always accessible to law enforcement. Scholars examining the international dimensions of cyber-offending emphasize that private actors often hold the most critical evidence but lack legal obligations to preserve or disclose it (Gundur et al., 2021). Some platforms may voluntarily cooperate with investigations, while others may resist due to privacy concerns, lack of trust in law-enforcement agencies, or conflicting jurisdictional requirements.

The multi-stakeholder nature of metaverse governance thus creates a complex matrix of authority. Platform operators shape rules and evidence availability; states attempt to enforce national laws; private server owners control local environments; and decentralized networks operate beyond centralized oversight. These overlapping jurisdictions create uncertainty about responsibility, accountability, and compliance. Scholars analyzing global governance emphasize that such fragmentation poses significant challenges for building coherent legal frameworks that protect users while respecting state sovereignty (Abbasi, 2023).

Conflicts of law represent a central challenge in prosecuting metaverse-based crimes. When users from different countries interact within borderless virtual environments, their conduct may fall under multiple, conflicting legal regimes. Determining which law applies requires courts to assess connections among the offender, the victim, the platform, the digital asset, and the infrastructure supporting the interaction. Scholars studying international cybercrime patterns argue that transnational digital interactions produce overlapping claims of jurisdiction that complicate enforcement and create opportunities for offenders to exploit inconsistencies (Gundur et al., 2021). These conflicts manifest in questions of attribution, responsibility, and extraterritorial enforcement.

Attribution of responsibility across jurisdictions becomes difficult when digital identities are fluid, decentralized, or anonymized. Scholars analyzing personal identity in immersive environments emphasize that avatars may reflect complex combinations of user behavior, system algorithms, and biometric inputs (Mitrushchenkova, 2023). This complexity undermines traditional attribution methods that rely on identifying devices, IP addresses, or physical proximity. If an avatar commits harmful actions in a virtual environment, it may be unclear whether the offender is physically located in one jurisdiction, using infrastructure in another, and causing harm in a third. Courts must determine which state has the primary connection to the offense and whether multiple jurisdictions may assert simultaneous authority.

Extraterritorial enforcement challenges arise when states attempt to prosecute offenses committed by individuals located abroad or whose actions are mediated through foreign platforms. Scholars examining international governance frameworks highlight that states often face resistance when seeking evidence from foreign companies, particularly when data are protected by privacy laws, corporate policies, or conflicting national regulations (Abbasi, 2023). For example, the European Union's GDPR imposes strict constraints on cross-border data sharing, potentially limiting access to evidence for investigations initiated outside the EU. Conversely, some states impose broad surveillance authorities that may conflict with the privacy obligations of multinational platforms.

Comparisons of approaches in the EU, US, China, and regional blocs reveal differing philosophical orientations toward digital governance. The EU emphasizes user rights, data protection, and platform accountability, creating robust regulatory frameworks that may conflict with more permissive jurisdictions. The US prioritizes innovation, free expression, and platform autonomy, resulting in weaker regulatory burdens on digital service providers. China's model emphasizes state control, data localization, and strict enforcement mechanisms. Scholars studying global variations in cybercrime victimization argue that these divergent approaches create regulatory friction that hinders coordinated enforcement across borders (Yarovenko et al., 2023). In Africa, Latin America, and Southeast Asia, emerging regulatory frameworks reflect diverse socio-political conditions, further complicating harmonization.

These legal divergences create conflicts in cases involving virtual property, digital identity, and avatar-based harm. For example, EU law may consider avatar manipulation a violation of privacy or personal dignity, while US law may treat it as a contractual violation rather than a criminal act. China may assert jurisdiction over any platform that engages Chinese users, even if the platform is hosted abroad. Such conflicts create legal uncertainty for victims, offenders, and investigators.

5. Forensic Approaches and Investigative Techniques

The forensic investigation of cybercrimes occurring within the metaverse demands a reconceptualization of digital forensics as traditionally practiced in two-dimensional online environments. Conventional forensic models evolved around static or semi-static digital artifacts—emails, chat logs, file metadata, browser records, IP addresses, device imaging, and server logs. These categories of evidence, although often complex, relied on established structures of data persistence, hierarchical storage, and relatively predictable communication patterns. The metaverse disrupts these assumptions by introducing immersive three-dimensional spaces, avatar-mediated actions, dynamic environmental rendering, decentralized assets, biometric input streams, and AI augmentation. The investigative process must therefore adapt to these multidimensional data forms, which are difficult to capture, preserve, authenticate, and present in legal proceedings. Scholars examining digital identity and emotional presence in immersive environments emphasize that forensic investigation must reflect the psychological realism and behavioral nuance of avatar interactions, which can mirror real-world encounters in both intensity and impact (González-Tapia, 2023). Similarly, research exploring personal identity construction in the metaverse demonstrates that the complexity of user behavior, system mediation, and representational fluidity requires highly sophisticated forensic strategies (Mitrushchenkova, 2023).

As a result, forensic approaches in the metaverse expand far beyond conventional cyber-investigation. They encompass immersive scene reconstruction, avatar behavioral analysis, blockchain forensics, NFT tracking, smart contract auditing, AI-driven detection models, biometric forensics, and complex cross-platform evidence collection. Additionally, investigators must navigate substantial challenges in collaborating with platform operators, who control the infrastructure, access to logs, interaction data, and system-level information needed for accurate forensic reconstruction. Scholars studying multi-stakeholder governance frameworks warn that private control of digital ecosystems creates significant asymmetries between law enforcement needs and platform incentives (Abbasi, 2023). These asymmetries shape forensic possibilities at every stage.

Digital forensics within immersive environments requires new tools, methodologies, and interpretive frameworks that can handle the spatial, behavioral, and real-time properties of metaverse activity. Unlike traditional digital platforms, which store relatively stable text, image, or network logs, immersive environments generate continuous, high-volume streams of spatialized data—avatar movement coordinates, interaction distances, collision events, gesture patterns, haptic feedback signals, gaze tracking vectors, and voice proximity indicators. These elements represent embodied interactions, reflecting not only what users did but how they navigated space, responded to environmental cues, and engaged emotionally with others. They serve as behavioral evidence that is essential for understanding intent, consent, threat, and harm in immersive contexts.

Immersive scene reconstruction is one of the most critical yet technically challenging components of metaverse forensics. In physical crime scenes, investigators reconstruct events by analyzing physical traces, spatial layout, witness testimonies, and contextual data. In traditional cybercrime, reconstruction involves mapping digital actions, correlating timestamps, and examining metadata. The metaverse blends both domains: investigators must reconstruct a three-dimensional virtual environment to understand the spatial and behavioral dimensions of the offense.

This process requires capturing or recreating the exact state of the virtual environment at the moment of the crime, including object placement, avatar positions, lighting conditions, environmental physics, and system-generated elements. Scholars examining technologically mediated abusive conduct note that harmful actions in immersive environments often depend heavily on spatial proximity, gesture realism, and embodied interaction cues (Sánchez, 2022). For example, if an avatar engages in non-consensual physical contact with another avatar, the evidentiary question is not simply whether two accounts interacted but how their avatars moved, what gestures were made, whether haptic systems were activated, and whether AI-generated responses contributed to the encounter.

However, immersive scenes are difficult to reconstruct due to the volatility of spatial data. Most platforms do not store full three-dimensional logs of every user interaction because doing so would require massive storage resources. Instead, platforms prioritize real-time rendering and performance optimization, often discarding intermediate frames or locally processed biometric inputs. Scholars studying emotional presence and behavioral realism in virtual environments emphasize that avatar gestures and micro-expressions—central to understanding intent—are often generated through a combination of sensor input and AI interpolation (González-Tapia, 2023). If the platform does not store such data, the forensic reconstruction becomes incomplete or speculative.

Reconstruction also requires alignment between different layers of evidence: motion-tracking data from user devices, server-side logs of interaction triggers, and environmental data from rendering engines. Because these layers may be generated by different systems, stored in different locations, or subject to different retention policies, investigators may lack access to integrated datasets. Scholars examining global cybercrime patterns stress that fragmentation of digital traces across distributed networks complicates efforts to rebuild event sequences, especially when offenders operate across jurisdictions (Gundur et al., 2021). Additionally, scene reconstruction may depend on cooperation from platform operators who control proprietary data, making the process vulnerable to corporate policies rather than forensic standards.

Avatar behavioral forensics is emerging as a new subfield that analyzes avatar movement, gesture patterns, voice interactions, gaze direction, and behavioral anomalies to determine user intent and identity. In immersive environments, avatars serve as proxies for individuals' embodied presence, and behavior analysis becomes a crucial evidentiary tool. Scholars exploring personal identity in the metaverse argue that avatars reflect not only user intention but also system mediation, algorithmic prediction, and biometric input, creating a complex interplay that must be carefully interpreted (Mitrushchenkova, 2023).

Behavioral forensics may involve analyzing:

- movement signatures (unique patterns of walking, gesturing, or interacting),
- proximity patterns (how closely an avatar approaches others),
- micro-gesture cues (hand movements, facial expressions),
- spatial awareness indicators (turning, looking, following),
- interaction triggers (object pickups, menu selections), and
- voice patterns (tone, emotional cues, timing).

These cues may help determine whether an avatar behaved aggressively, coercively, deceptively, or defensively. For example, if an offender stalks a victim's avatar across multiple virtual environments, movement-path reconstruction and proximity analysis can reveal persistent pursuit. Scholars examining socio-economic cybercrime vulnerabilities emphasize that behavioral patterns can reveal power dynamics, exploitation strategies, and identity deception tactics used by offenders in complex digital spaces (Yarovenko et al., 2023).

However, behavioral forensics faces multiple challenges. System-generated animations—used to smooth avatar movements or compensate for missing biometric data—may distort the true actions of the user. AI-assisted gesture prediction may alter behavior in subtle ways. Voice chat systems may apply filters, spatialization effects, or voice-masking features that complicate speaker identification. The potential for deepfake impersonation or avatar spoofing further complicates attribution, as attackers may replicate another user's avatar to commit harmful acts. Scholars examining image-based violence and impersonation emphasize that identity manipulation is particularly problematic in digital ecosystems lacking strong authentication or biometric protections (Sánchez, 2022).

Thus, avatar behavioral forensics must incorporate advanced verification frameworks, including cross-referencing device logs, biometric signatures, and motion-capture data to authenticate user actions. Investigators must distinguish between authentic user-generated behavior, AI-assisted movement, and spoofed or manipulated interactions.

As the metaverse increasingly relies on decentralized economies, blockchain and NFT forensics have become essential components of investigative practice. Virtual assets—land, avatars, objects, skins, artwork, currency, and collectibles—are frequently stored as tokens on blockchain networks. While blockchain's immutability and transparency create an evidentiary advantage, its pseudonymity and decentralization make attribution difficult. Scholars examining metaverse legal structures highlight that tokenized property introduces significant ambiguity concerning ownership, consent, and contractual obligations (Kasiyanto & Kilinc, 2022). These ambiguities shape how forensic systems must analyze blockchain interactions.

Tracking ownership of digital assets requires investigators to correlate blockchain transactions with platform-level interactions. Blockchain records show asset transfers but do not reveal platform context, user identity, or the meaning of the transaction within the immersive environment. For example, if an NFT representing virtual land is transferred to a new address without the owner's consent, the blockchain will show the transfer, but investigators must analyze platform records to determine how the transfer was initiated. Scholars examining international cyber-offending emphasize that attackers often combine social-engineering tactics, platform manipulation, and blockchain transfers to hide illicit conduct (Gundur et al., 2021).

Investigators must therefore link three data layers:

- blockchain transaction logs,
- platform interaction logs, and
- user device activity.

This linkage is difficult when platform operators restrict access to logs or when blockchain networks incorporate privacy features such as mixers or zero-knowledge proofs. However, blockchain's transparency also offers forensic advantages. Once investigators identify a malicious wallet address, they can track its transaction history indefinitely. Scholars analyzing transnational cybercrime victimization argue that blockchain analysis is crucial for identifying patterns of exploitation and movement of stolen digital goods across borders (Yarovenko et al., 2023).

Smart contracts govern many metaverse transactions, including asset transfers, rental agreements, event participation, and governance functions. Forensic analysis must therefore include code auditing, event log examination, and identification of vulnerabilities exploited by attackers. Scholars studying digital governance emphasize that smart-contract exploits often arise from poorly implemented code, inadequate auditing, or unforeseen interactions between contract functions (Abbasi, 2023). Attackers may encode malicious logic, manipulate contract states, or trigger reentrancy vulnerabilities to steal assets.

Smart contract forensics involves reviewing:

- contract source code,
- constructor parameters,
- emitted events,
- function-call histories,
- dependency libraries, and
- blockchain state changes.

Investigators must determine whether the exploit involved user error, code-based vulnerabilities, or platform-level negligence. Additionally, smart contracts often operate across multiple jurisdictions and may involve governance policies determined by decentralized communities. This creates legal uncertainty regarding liability, intent, and recovery of stolen assets.

AI-driven forensic tools play a central role in detecting behavioral anomalies, identifying identity manipulation, and automating evidence analysis in the metaverse. Because immersive environments generate large quantities of data, manual investigation is impractical. Machine learning models can analyze motion patterns, gaze trajectories, asset-transfer histories, interaction frequency, and anomaly detection signals to flag suspicious behavior. Scholars examining technologically mediated harm note that AI systems influence both user behavior and forensic interpretation, creating opportunities for automated identification of manipulative or coercive behaviors (González-Tapia, 2023).

Anomaly detection models can identify unusual avatar movements, unexpected asset transfers, suspicious proximity patterns, or inconsistent gesture data. For example, if a user typically moves with a consistent motion signature but suddenly exhibits movement patterns inconsistent with their typical behavior, it may indicate account compromise or avatar spoofing. Scholars studying cybercrime strategies argue that attackers often rely on pattern deviation when engaging in criminal activity, making behavioral anomaly detection a powerful forensic tool (Gundur et al., 2021).

Machine-learning models can also detect coordinated behavior across multiple avatars, such as swarm attacks, harassment campaigns, or bot-driven manipulation. Models trained on normal interaction patterns can identify irregularities that deviate from community norms, providing early-warning signals.

Identity verification is one of the most challenging aspects of metaverse forensics. Avatars may be customized extensively, biometric inputs may be minimal, and attackers may create highly convincing deepfake avatars. Scholars analyzing personal identity in immersive worlds emphasize that identity representation is fluid, hybrid, and technologically mediated, complicating verification (Mitrushchenkova, 2023).

AI-based verification tools cross-reference:

- voice signatures,
- motion-capture patterns,
- gaze-tracking characteristics,
- biometric markers (if available), and
- device-level identifiers.

These tools can help determine whether an avatar is controlled by its rightful owner. However, attackers may attempt to bypass verification systems using biometric replay attacks, synthetic behavioral data, or AI-generated impersonation.

One of the most significant barriers to effective metaverse forensics is the difficulty of obtaining necessary data from platform operators. Investigators rely heavily on platforms for access to interaction logs, device data, network records, and environmental snapshots. However, platform governance structures are private, profit-driven, and often transnational. Scholars examining cybercrime justice systems highlight that dependence on private intermediaries undermines state capacity and creates systemic obstacles in digital investigations (Brants et al., 2020).

Platforms often limit data access due to privacy policies, corporate liability concerns, cost, and technical constraints. Some store only limited logs; others encrypt or anonymize data; still others routinely delete records to reduce storage costs. Scholars examining global digital governance warn that fragmented data policies create significant asymmetries in investigative power across countries (Abbasi, 2023).

Conflicts between platform autonomy and law enforcement authority frequently arise. Platforms may resist data requests due to jurisdictional conflicts, privacy obligations, or fear of setting legal precedents. Scholars studying legal fragmentation in decentralized systems argue that platform-led governance often supersedes state enforcement, creating gaps in accountability (Kasiyanto & Kilinc, 2022). These gaps hinder timely investigations, disrupt evidence collection, and create environments where offenders exploit jurisdictional ambiguity.

6. Comparative Legal Analysis

The emergence of the metaverse has forced legal scholars, regulators, and governments to reassess how cybercrime frameworks operate in an ecosystem defined by digital embodiment, decentralized structures, and transnational interactions. Traditional legal systems were developed in an era when harmful conduct occurred either in physical spaces or through comparatively simple digital interfaces such as emails, websites, and messaging platforms. The metaverse radically reconfigures this landscape by introducing immersive spaces in which avatars act as proxies for users, blockchain-based economies govern the movement of digital property, and AI systems shape behavioral interactions. As a result, national and international legal regimes struggle to apply existing cybercrime doctrines to immersive environments, exposing significant doctrinal gaps, enforcement inconsistencies, and regulatory fragmentation. Scholars examining global cybercrime patterns emphasize that the complexity of transnational digital ecosystems has already strained legal systems, and the metaverse intensifies these pressures by adding layers of psychological realism, biometric surveillance, and decentralized data flows that undermine traditional jurisdictional anchors (Gundur et al., 2021).

To evaluate how legal systems currently address metaverse-based offenses, it is necessary to examine national cybercrime frameworks, international conventions, and the structural gaps that emerge when these frameworks confront immersive digital environments. While many legal systems regulate hacking, fraud, identity theft, stalking, harassment, and digital property crimes, these laws were not designed to address avatar-based harm, real-time spatial interactions, deepfake impersonation, NFT theft, smart contract manipulation, or biometric-data violations. Additionally, because the metaverse dissolves geographical boundaries, mechanisms for cross-border cooperation—already strained in traditional cybercrime investigations—are even less effective in immersive contexts. Scholars observing the fragmentation of digital governance warn that when private platforms and decentralized infrastructures assume governance roles traditionally filled by states, legal coherence becomes difficult to achieve (Abbasi, 2023).

Against this backdrop, a comparative legal analysis reveals deep tensions between the assumptions embedded in national cybercrime laws and the reality of metaverse interactions. These tensions are evident across three core dimensions: how national frameworks currently apply or fail to apply; what role international conventions play in promoting harmonization; and where major structural gaps exist that hinder effective prosecution of metaverse-based crimes.

National cybercrime frameworks around the world were designed to address offenses involving unauthorized access, data interference, system disruption, digital fraud, identity theft, and cyberstalking. These categories align with traditional digital infrastructures such as websites, email systems, online banking, and two-dimensional communication platforms. In many countries, these laws were drafted in the late 1990s or early 2000s, long before the emergence of immersive virtual worlds, avatar-based interactions, decentralized digital assets, or biometric-driven VR platforms. As a result, national frameworks often apply poorly—sometimes not at all—to metaverse-based conduct.

Many existing cybercrime laws define harmful conduct in terms of unauthorized access to computer systems, data manipulation, or interference with informational content. However, the metaverse shifts the locus of harmful conduct from informational units to embodied interactions. For example, avatar-based harassment, unwanted virtual touching, forced proximity, or stalking often depend on three-dimensional behavior rather than textual or informational exchanges. Scholars studying emotional harms in immersive environments emphasize that the psychological intensity of avatar interactions often mirrors physical encounters, raising questions about whether traditional harassment or assault statutes can accommodate these new forms of harm (González-Tapia, 2023). Yet many national frameworks do not criminalize avatar-based conduct unless it involves explicit threats, sexually explicit content, or discriminatory messaging.

Similarly, virtual property crimes often fall outside traditional cybercrime laws. In many jurisdictions, theft requires the unlawful taking of tangible property or financial instruments. Digital assets in the metaverse—NFTs, skins, virtual land, virtual structures, and tokenized objects—may not fit the legal definition of property, especially when they exist on decentralized blockchain networks. Scholars analyzing the legal ambiguities of tokenized property highlight that jurisdictions differ widely in whether they recognize NFTs and digital tokens as property, contract rights, securities, or intangible assets (Kasiyanto & Kilinc, 2022). As a result, when attackers steal metaverse property by manipulating smart contracts or hacking user accounts, prosecutors often struggle to classify the offense within existing legal categories. Some jurisdictions treat it as a form of fraud, others as unauthorized access, and others decline to pursue the offense due to definitional uncertainty.

Identity-related offenses also challenge national frameworks. Many cybercrime laws prohibit impersonation, identity theft, or misuse of personal identifiers. In the metaverse, however, identity is mediated through avatars, biometric inputs, motion-capture signatures, and digital customizations. When attackers clone an avatar, hijack an account, or deploy a deepfake version of a user's avatar, national laws may not recognize these actions as identity theft unless the offender uses legally recognized personal information. Scholars examining metaverse identity formation argue that avatars represent a complex blend of psychological projection, digital embodiment, and social representation (Mitrushchenkova, 2023). Yet laws that protect identity typically rely on physical-world constructs such as names, birthdates, social security numbers, or financial identifiers, leaving avatar identity manipulation unaddressed.

Biometric-data theft in immersive environments presents another challenge. VR and AR devices collect vast amounts of biometric data, including eye-tracking information, facial expressions, voice signatures, hand-motion vectors, emotional states, and reaction-time profiles. Scholars investigating immersive environments highlight that this data not only influences user experience but can be used by attackers to create deepfake avatars, manipulate behavior, or access accounts (González-Tapia, 2023). However, many national cybercrime laws do not explicitly protect biometric data collected through consumer devices unless the jurisdiction has enacted privacy or data-protection statutes. Even in regions with strong biometric protections, such as the European Union, immersive-environment biometric data may fall into ambiguous categories if it is processed locally on devices or transmitted through decentralized architectures.

Social engineering in immersive environments likewise exposes limitations in national frameworks. In many jurisdictions, social engineering attacks are prosecuted under fraud or deception laws. However, the tactics used in metaverse spaces—avatar-based impersonation, emotionally manipulative gestures, AI-generated authority cues, proximity-based persuasion—are far more immersive than the textual phishing or email-based deception that these laws originally targeted. Scholars examining international cyber-offending emphasize that immersive environments create new opportunities for manipulation because users respond to embodied cues that mimic real-world social behavior (Gundur et al., 2021). Yet national frameworks have not been updated to include immersive behavioral manipulation as a form of criminal deception.

Harassment, stalking, and intimidation laws also exhibit gaps when applied to metaverse interactions. Traditional statutes focus on unwanted communication, physical pursuit, or real-world threats. In the metaverse, avatar stalking may involve following users across virtual environments, invading virtual personal space, or engaging in repeated unwanted proximity behaviors that mimic physical pursuit. Scholars studying image-based and psychologically mediated harm emphasize that these behaviors can create significant emotional distress, especially given the immersive and embodied nature of metaverse interactions (Sánchez, 2022). Yet many jurisdictions do not recognize avatar-based proximity behaviors as legally salient.

Finally, national frameworks often rely on the assumption that digital evidence resides within territorial boundaries. Many statutes require that logs, IP addresses, or digital artifacts be accessible through national warrants, subpoenas, or service-provider obligations. The metaverse fundamentally disrupts these assumptions by distributing evidence across decentralized networks, private platforms, and multinational cloud infrastructures. Scholars studying global governance and platform power caution that private companies may not comply with national orders if doing so conflicts with corporate policy, foreign law, or user privacy protections (Abbasi, 2023). This disconnect leaves national cybercrime frameworks ill-equipped to handle investigations that require cross-border data retrieval, platform cooperation, or blockchain-state analysis.

Overall, existing national cybercrime laws apply imperfectly to the metaverse. While some offenses can be shoehorned into existing categories, many forms of harm, manipulation, identity interference, and digital property violation fall outside traditional definitions. This mismatch underscores the need for legislative reform that explicitly addresses the embodied, decentralized, and transnational nature of metaverse interactions.

International conventions serve as critical tools for harmonizing legal definitions, enabling cross-border cooperation, and facilitating evidence sharing. The most influential of these conventions—particularly the Budapest Convention on Cybercrime—provides mechanisms for mutual assistance, procedural powers, definitions of cyber offenses, and frameworks for international cooperation. However, the Budapest Convention and other digital governance agreements were drafted before the emergence of immersive, decentralized environments. As a result, significant gaps remain between the conventions' scope and the realities of metaverse-based criminality.

The Budapest Convention focuses on offenses involving unauthorized access, data interference, system interference, computer-related fraud, child exploitation, and procedural powers for evidence collection. These categories remain relevant in the metaverse, as many offenses involve unauthorized access to accounts, manipulation of digital assets, or fraud conducted through decentralized environments. However, the Convention does not explicitly address issues such as avatar-based harm, biometric-data exploitation, deepfake impersonation, or smart-contract manipulation. Scholars analyzing the narrative framing of cybercrime emphasize that existing conventions rely on assumptions about data stability, authentication mechanisms, and communication formats that do not align with the volatility and behavioral realism of immersive environments (Brants et al., 2020).

Regional governance frameworks—such as those developed within the European Union, ASEAN, the African Union, and various Latin American coalitions—address digital privacy, cybersecurity standards, and cross-border cooperation. Yet these, too, were not designed with the metaverse in mind. Scholars examining socio-economic cybercrime disparities argue that regions with lower digital literacy or limited regulatory capacity face greater risks in immersive spaces, making harmonization even more necessary (Yarovenko et al., 2023). But harmonization is difficult when metaverse interactions rely on private governance structures that are not directly accountable to international bodies.

The metaverse also complicates the applicability of data-sharing provisions in international conventions. Many conventions rely on mutual legal assistance treaties (MLATs) as mechanisms for cross-border data retrieval. However, MLAT processes are slow and bureaucratic, and the speed of metaverse interactions makes delayed evidence collection highly problematic. Scholars studying decentralized digital ecosystems emphasize that evidence in such environments is ephemeral and may disappear or mutate before MLAT procedures can retrieve it (Alruwaili, 2021). Furthermore, decentralized ledgers, smart contracts, and distributed networks may not respond to MLAT requests because there is no central authority capable of compliance.

International conventions also fail to address conflicts between private platform governance and state authority. Platforms may decline to cooperate with international requests, citing corporate policy, jurisdictional limitations, or user privacy obligations. Scholars examining governance asymmetries argue that the metaverse strengthens the power of private actors, making international conventions less effective unless they include explicit obligations for platform operators (Abbasi, 2023).

Across national and international legal frameworks, several structural gaps hinder effective regulation, investigation, and prosecution of metaverse-based crime. The most fundamental of these gaps is the absence of metaverse-specific criminal definitions. Existing laws do not recognize avatar-based behaviors as harmful conduct unless they involve explicit threats or prohibited content. Scholars studying emotional harm in immersive environments stress that avatar-based contact can produce real psychological injury, yet legal systems have not evolved to reflect the embodied nature of immersive interactions (González-Tapia, 2023).

Another major gap involves insufficient mechanisms for cross-border prosecution. Because the metaverse dissolves geographical boundaries, offenders often operate across jurisdictions in ways that evade national authority. Scholars analyzing fragmented governance structures emphasize that traditional enforcement mechanisms—territorial warrants, service-provider obligations, and MLAT procedures—are too slow and territorially bound to address crimes that occur in decentralized environments (Kasiyanto & Kilinc, 2022). Without new frameworks for real-time, cross-jurisdictional evidence collection, offenders will continue to exploit jurisdictional gaps.

Private platform governance creates another significant gap. Because metaverse environments are controlled by companies rather than states, evidence availability depends on corporate policy rather than legal obligation. Scholars examining private governance identify this as a source of legal fragmentation that undermines accountability, enforcement, and user protection (Abbasi, 2023). When platforms retain exclusive control of logs, user data, and behavioral records, states lack the ability to enforce cybercrime laws effectively.

Identity verification is also inadequately addressed in current legal systems. Traditional identity laws assume stable personal identifiers, but metaverse identity is fluid, customizable, and technologically mediated. Scholars analyzing identity construction in immersive environments warn that avatar manipulation and deepfake impersonation pose unique risks that are not captured by existing identity-theft statutes (Mitrushchenkova, 2023).

Decentralized digital assets introduce further gaps. Many jurisdictions lack clear rules governing NFT ownership, smart-contract liability, or blockchain-based fraud. Scholars studying the legal ambiguity of tokenized metaverse property emphasize that inconsistent legal classifications across countries create substantial enforcement difficulties and allow offenders to exploit regulatory arbitrage (Kasiyanto & Kilinc, 2022).

Taken together, these gaps illustrate why existing legal systems face profound challenges when addressing immersive, decentralized, and transnational metaverse-based crimes.

7. Conclusion

The rapid emergence of the metaverse as a multidimensional digital ecosystem profoundly challenges long-standing assumptions in criminal law, evidence, and jurisdiction. Unlike earlier forms of cyberspace, the metaverse operates as an embodied, persistent, and immersive environment where users interact through avatars, transact through decentralized assets, and participate in social, economic, and cultural systems that transcend territorial borders. This transformation redefines the nature of criminal behavior, producing new categories of harm that do not fit within the conceptual boundaries of traditional cybercrime. It also creates a digital environment where conduct is experienced as real, immediate, and psychologically impactful, necessitating an evolution in how law understands agency, consent, identity, and victimization in virtual spaces.

The evidentiary implications of this shift are far-reaching. Traditional digital forensics relies on stable logs, textual communication, and metadata trails that reflect discrete actions within a recognizable architecture. In contrast, immersive environments generate vast amounts of volatile, real-time spatial data that are usually processed locally, modified by artificial intelligence, or discarded altogether. Investigators must reconstruct scenes that may no longer exist, interpret avatar movements that may blend user intent with AI interpolation, and analyze biometric cues that are rarely stored in accessible form. These challenges demand new forensic approaches capable of capturing and interpreting three-dimensional interactions, behavioral signatures, and decentralization-driven traces. Without such innovations, many metaverse-based offenses will remain difficult to verify, prosecute, or even detect.

Jurisdictional complexity further complicates legal enforcement. The metaverse dissolves the geographic anchors that historically defined criminal authority, creating environments where offenders, victims, servers, and platform operators may all be located in different parts of the world. This dispersion breaks the connection between territoriality and legal responsibility, making it increasingly difficult for any single jurisdiction to claim authority. In addition, platform operators and private actors often control the critical data required for investigations, yet they operate according to internal policies shaped by business interests rather than legal imperatives. As a result, states frequently lack direct access to essential information and must rely on voluntary cooperation mechanisms that are inconsistent, slow, and unpredictable.

Efforts to find guidance in international law reveal additional limitations. Existing conventions and regional agreements were developed for a previous generation of cybercrime and do not explicitly address the complexities of immersive environments, decentralized assets, or AI-mediated identity manipulation. Mechanisms such as mutual legal assistance treaties—already slow and bureaucratic—are poorly suited for real-time digital ecosystems in which evidence may disappear in seconds. Harmonizing legal standards across borders remains difficult, especially given the divergent regulatory philosophies of different states and the growing influence of private governance frameworks that operate outside traditional legal structures.

Legal gaps are therefore widespread and systemic. National frameworks lack metaverse-specific definitions of harm, leaving avatar-based assault, stalking, coercion, and harassment in uncertain doctrinal territory. Identity-related crimes become increasingly difficult to classify when avatars can be cloned, deepfaked, or manipulated without relying on traditional personal identifiers. Digital property crimes involving NFTs, virtual land, and tokenized objects highlight contradictions in how jurisdictions classify intangible assets. The absence of harmonized regulations for blockchain ecosystems, smart contracts, and decentralized governance structures leaves victims with limited recourse and investigators with constrained procedural authority. Without comprehensive reform, these gaps will continue to allow offenders to exploit digital spaces with minimal risk.

The path forward requires a re-imagining of criminal law and digital governance that aligns with the realities of spatial computing and immersive interaction. Legal frameworks must expand to recognize the embodied nature of virtual presence, the psychological intensity of avatar-mediated harm, and the hybrid forms of identity that users inhabit. Forensic science must evolve to capture volatile spatial data, reconstruct complex interactions, authenticate digital behavior, and integrate decentralized transactional records. Jurisdictional doctrine must adapt to environments in which territoriality is no longer the primary determinant of authority, favoring flexible models capable of allocating responsibility across multiple stakeholders. International cooperation mechanisms must become faster, more interoperable, and more attuned to the technical architectures of decentralized digital ecosystems.

Ultimately, addressing cybercrime in the metaverse requires an interdisciplinary approach that brings together law, computer science, behavioral psychology, blockchain analytics, and platform governance. As immersive environments become more pervasive, societies will need legal structures that not only respond to emerging harms but also anticipate them. A failure to modernize criminal justice systems will leave users vulnerable, weaken public trust, and allow virtual spaces to become fertile grounds for exploitation. Creating a resilient legal and forensic framework for the metaverse is therefore essential for ensuring that the future of digital interaction remains safe, accountable, and just.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abbasi, O. (2023). The Role of the United Nations in Organizing the Work of the Metaverse. *Law*, *2*(3), 205-234. https://doi.org/10.59759/law.v2i3.292

Alruwaili, F. F. (2021). CustodyBlock: A Distributed Chain of Custody Evidence Framework. *Information*, *12*(2), 88. https://doi.org/10.3390/info12020088

Brants, C., Johnson, D., & Wilson, T. (2020). New Wine in Old Bottles: Alternative Narratives of Cybercrime and Criminal Justice? *The Journal of Criminal Law*, *84*(5), 403-406. https://doi.org/10.1177/0022018320952555

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

Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y. C., & Mejía, D. D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. https://doi.org/10.21428/cb6ab371.5f335e6f

Kasiyanto, S., & Kilinc, M. R. (2022). Legal Conundrums of the Metaverse. *Journal of Central Banking Law and Institutions*, *1*(2). https://doi.org/10.21098/jcli.v1i2.25

Mitrushchenkova, A. N. (2023). Personal Identity in the Metaverse: Challenges and Risks. *Kutafin Law Review*, *9*(4), 793-817. https://doi.org/10.17803/2313-5395.2022.4.22.793-817

Sánchez, A. R. (2022). Situacion De Abuso Sexual Basado en Imagenes en Mexico Entre 2017 Y 2018 (Imaged-Based Sexual Abuse in Mexico Between 2017 and 2018). *Universos Jurídicos*(18), 1-22. https://doi.org/10.25009/uj.vi18.2621

Yarovenko, H., Łopatka, A., Vasilyeva, T., & Vida, I. (2023). Socio-Economic Profiles of Countries - Cybercrime Victims. *Economics & Sociology*, *16*(2), 167-194. https://doi.org/10.14254/2071-789x.2023/16-2/11