

Article

Facing Crimes in the Metaverse – The Uprising of Digital Deviance and the Crisis of Regulation

Abdelwahab Mansour Alenezi^{1,*} Muaath Suleiman Almulla²¹ KICRA – Kuwait Institute for Criminal Research & Analysis, Shuwaikh Industrial, Kuwait² Criminal Law, Kuwait International Law School (KILAW), Doha, Kuwait*** Corresponding author:** Abdelwahab M. Alenezi, wmalenezi@outlook.com**CITATION**

Alenezi A, Almulla M. Facing Crimes in the Metaverse – The Uprising of Digital Deviance and the Crisis of Regulation. *Metaverse*. 2026; 7(2):8291. <https://doi.org/10.54517/m8291>

ARTICLE INFO

Received: 7 November 2025

Accepted: 30 March 2026

Available online: 15 April 2026

COPYRIGHT

Copyright © 2026 by author(s).

Metaverse is published by Asia Pacific Academy of Science Pte. Ltd. This work is licensed under the Creative Commons Attribution (CC BY) license. <https://creativecommons.org/licenses/by/4.0/>

Abstract: It seems that humans have gone too far in creating technological industries; it also seems that they have lost control over the ethics of developing their various tools. If the legal system in the past faced a major challenge in protecting the rights and interests of those dealing with the Internet from the misuse of information-technology tools, it now faces a new challenge after Mark Zuckerberg's announcement (owner of Facebook, which changed its name to "Meta Platforms") of his commitment to developing the virtual world he called "Metaverse" – a world that blends reality and fantasy, allowing users to interact with one another with real emotions in three-dimensional virtual environments completely similar to reality. This paper aims to define the nature of metaverse technology and study the extent to which criminal laws are prepared to face the challenges it poses, especially with the emergence of criminal activities through it. To this end, the research followed a descriptive and analytical approach in presenting the topic and was divided into three parts: Firstly, explaining the nature of metaverse technology. Secondly, Describing examples of attacks in this environment. Lastly, Addressing the extent to which criminal laws are prepared to face the challenges of metaverse technology. The research concluded that the metaverse is a recent phenomenon in the cyberspace environment, which began through the electronic-gaming portal and has become a business environment in various fields through blockchain platforms and non-fungible tokens (NFTs). Avatars are a form of personal data that identify users for access to the metaverse and may themselves become the subject or tool of criminal activities. The paper also found that the danger lies in the uncontrolled acceleration of technological development. The metaverse, without legal safeguards, is fertile ground for numerous crimes. Criminal activities in the metaverse are modeled on cybercrimes given their nature and characteristics. Consequently, the research recommends that legislators review substantive and procedural laws to ensure effective responses at both international and national levels, to adopt the idea of electronic legal personality, and to refrain from rushing to introduce practices and services in this environment until clear legal frameworks define obligations and responsibilities.

Keywords: Metaverse technology, Cybercrime, Criminal law, Virtual activities, Digital legal personality, Avatar.

1. Introduction

1.1 Research background

Rapid technological innovation has reshaped social, economic, and legal systems, making digital interaction indispensable. However, the same acceleration has enabled immersive environments- most notably the metaverse where human conduct, identity, and harm may unfold beyond traditional physical boundaries.

The metaverse may be described as a next-generation internet layer that blends

virtual and augmented reality into persistent, immersive environments where users interact through digital identities. Global attention intensified after major industry announcements in 2021, accelerating adoption and investment across multiple sectors.

Reports such as ESCWA highlight the metaverse's transformative potential while cautioning against ethical, legal, and security gaps [1]. These gaps may amplify familiar online risks in more immersive forms, intensifying challenges related to identity, data, and accountability.

1.2 Research problem

This study examines whether existing criminal law frameworks substantive and procedural are sufficiently equipped to address offenses committed within the metaverse. Criminal justice systems designed for tangible acts and physical harms face difficulties in defining offenses, attributing responsibility, and imposing sanctions in an environment where actions are virtual yet their impacts may be real.

1.3 Research significance

The significance of this research lies in recognizing that the metaverse is not merely a technological innovation but a legal and philosophical turning point. It pressures foundational criminal law concepts act, intent, harm, identity, evidence, and jurisdiction thereby raising urgent questions about accountability, data protection, and digital right. The study is therefore relevant to legislators, practitioners, and law-enforcement agencies seeking to adapt criminal governance to immersive digital environments.

1.4 Research Objectives

This paper aims to: (i) clarify the metaverse's defining characteristics as a technological and social architecture; (ii) identify emerging forms of criminal activity within immersive environments; (iii) assess the readiness of existing substantive and procedural criminal law to address such conduct; and (iv) propose legal and policy reforms to strengthen protection, accountability, and justice as the boundary between physical and virtual life becomes increasingly blurred.

1.5 Original Contribution of the Study

This paper makes three original contributions to the existing literature on metaverse-related cybercrime. First, it moves beyond descriptive accounts of virtual offenses by systematically distinguishing between deficiencies in substantive criminal law and procedural enforcement mechanisms within immersive environments. Second, unlike prior studies that focus primarily on avatars or isolated digital harms, this research conceptualizes the metaverse as a hybrid legal space where identity, conduct, and harm converge, thereby requiring a reconfiguration of traditional criminal law doctrines. Third, the paper offers a regionally grounded legal analysis by addressing the underexplored Arab legal context, bridging global academic debates with jurisdictions that remain largely governed by general cybercrime statutes rather than metaverse-specific regulation.

2. Literature review

The emergence of the metaverse has generated a rapidly expanding body of scholarship across law, technology, ethics, sociology, and economics. Legal research, in particular, has begun to question whether traditional regulatory and criminal law frameworks remain adequate for addressing the social, ethical, and criminal implications of immersive virtual environments.

Early conceptual works, such as those by Ashraf Mohamed Zidan and Saif Al-Suwaidi (2022) [2], describe the metaverse as a continuous digital space integrating physical and virtual experiences through immersive technologies. These studies emphasize its potential for social interaction and commercial innovation, while simultaneously warning of its capacity to facilitate new forms of manipulation and deviant behavior.

Similarly, Salah El-Din Hassan El-Sisi (2022) [3] situates the metaverse within the broader trajectory of technological dominance, arguing that the expansion of immersive digital environments has reached a critical ethical threshold where human values risk subordination to artificial systems.

From a legal perspective, Khaled Mamdouh Ibrahim (2023) [4] examines the adaptability of criminal and civil law frameworks to metaverse technologies. He conceptualizes the metaverse as a legal space that disrupts established notions of identity, ownership, and responsibility, advocating for the legal recognition of avatars and digital assets such as non-fungible tokens (NETs) as extensions of personal data subject to ownership, transfer, and infringement.

At the international level, reports by Elliptic (2022) [5] and assessments conducted by Interpol (2022) [6] highlight the metaverse's susceptibility to financial crimes, fraud, and digital exploitation. These reports emphasize how blockchain decentralization and user anonymity complicate investigation, attribution, and accountability within immersive environments.

The European Union has begun addressing these concerns through instruments such as the General Data Protection Regulation (GDPR) and ongoing initiatives on digital identity and virtual assets, positioning Europe among the legally prepared regions for emerging forms of virtual governance.

Foundational academic contributions by Susan W. Brenner (2008) [7,8] and Ben Chester Cheong (2022) [9] provide early and contemporary analyses of virtual crime. Brenner's concept of "fantasy crime" anticipated the psychological and legal dilemmas arising when actions in simulated environments produce real emotional or social harm, while Cheong expands this discussion by examining the legal status of avatars, intellectual property, and digital ownership within the metaverse.

From a criminological standpoint, scholars such as Simon Mackenzie (2022) [10] and Irina Filipova (2023) [11] frame the metaverse as an emerging frontier for deviance and financial misconduct. Their work links cryptocurrency fraud, virtual economies, and socially engineered crimes to broader transformations in digital market structures.

Collectively, this literature converges on the view that the metaverse represents more than a technological innovation; it constitutes a profound legal and social challenge. Its immersive, decentralized, and transnational architecture undermines traditional jurisdictional boundaries and evidentiary rules.

However, despite significant international and interdisciplinary engagement, a notable gap persists in Arabic legal scholarship. While Western and Asian studies increasingly propose frameworks for digital personality and virtual accountability, most Arab legal systems continue to rely on general cybercrime statutes that do not explicitly address offenses occurring within immersive or mixed-reality environments.

This paper seeks to bridge that gap by situating metaverse-related criminal challenges within an Arab legal perspective, while remaining aligned with international standards. By connecting global academic debates with regional legal realities, the study contributes a balanced framework for understanding how criminal

law may evolve to address ethical and criminal dimensions of life in the metaverse.

3. Methodology

3.1 Research design

This paper employs a descriptive and analytical approach to examine the phenomenon of Metaverse technology and its implications for criminal law. The descriptive aspect of the research is used to define the concept of the Metaverse, explain its technological mechanisms, identify its distinctive characteristics, and outline both its advantages and disadvantages. Through this, the paper provides a clear conceptual foundation for understanding how the Metaverse operates as a technological and social environment that enables real-time interaction through virtual identities.

The analytical component of the research is then applied to evaluate and interpret the emerging risks and criminal behaviors that take place within the Metaverse. By analyzing examples of attacks and violations occurring in virtual spaces, ranging from incitement, harassment, and identity manipulation to fraud, intellectual property infringement, and financial crimes; the paper seeks to determine the extent to which these activities challenge the established rules and principles of criminal law.

The methodology integrates comparative legal analysis by referencing relevant international reports, academic literature, and cybercrime legislation from different jurisdictions, particularly focusing on European, American, and Arab legal systems. This comparative perspective allows for identifying areas of convergence and divergence in how laws approach digital crimes and virtual accountability.

3.2 Selection criteria

The selection of legal systems, reports, and examples in this study was guided by three criteria. First, jurisdictions were chosen based on their regulatory engagement with digital governance and cybercrime, particularly within the European Union and the United States. Second, international reports were selected for their institutional credibility and relevance to metaverse-related risks, including publications by Interpol, Europol, and blockchain analytics organizations. Third, Arab legal systems were examined to highlight regulatory gaps in jurisdictions where immersive virtual environments remain governed by general cybercrime legislation rather than specialized frameworks.

3.3 Database Sources and Search Parameters

To ensure transparency and reproducibility, the following databases and sources were systematically consulted during the literature and legal review phase of this study:

Academic literature was retrieved from Google Scholar, Scopus, HeinOnline, and JSTOR. Legal instruments, legislative texts, and official policy documents were sourced from EUR-Lex (European Union law database), the United Nations Treaty Collection, official national legislative portals (including the UAE, Kuwait, and Saudi Arabia), and the Council of Europe Treaty Office. Institutional and grey literature reports were retrieved directly from the official websites of Interpol, ENISA, FATF, Elliptic, and Chainalysis.

The following keyword combinations and search strings were employed across the above databases:

"metaverse" and "criminal law"; "metaverse" and "cybercrime"; "virtual reality" and "criminal liability"; "avatar" and "legal personhood" or "digital identity"; "NFT"

and "fraud" or "money laundering"; "blockchain" and "financial crime" or "regulatory enforcement"; "virtual assault" and "criminal law"; "cybercrime jurisdiction" and "cross-border enforcement"; "digital evidence" and "immersive environment"; "Arab cybercrime law" or "Gulf cybercrime legislation"; "electronic legal personality" and "artificial intelligence."

Boolean operators (and, or) were applied consistently to refine search results. Searches were conducted in both English and Arabic to capture relevant scholarship and legislative material from Arab jurisdictions.

The review covered materials published or enacted between **2008 and 2023**. The year 2008 was selected as the lower boundary because it corresponds to the earliest peer-reviewed scholarship directly addressing criminal conduct in virtual environments (Brenner, 2008)[7]. The upper boundary of 2023 reflects the most recent institutional reports and academic contributions available at the time of writing. Foundational legal instruments predating this window, such as the Council of Europe's Budapest Convention on Cybercrime (2001) and the European Parliament's 2017 resolution on civil law rules on robotics, were included where directly relevant to the study's analytical framework, notwithstanding their earlier publication dates.

Sources were included if they met at least one of the following criteria: (i) they addressed legal, criminological, or ethical dimensions of virtual or immersive digital environments; (ii) they proposed or analyzed regulatory frameworks applicable to cybercrime or digital assets; or (iii) they represented authoritative institutional positions on metaverse-related risks. Sources were excluded if they were purely technical in nature without legal or policy implications, or if they could not be verified through an accessible institutional or academic repository.

Overall, the study combines descriptive mapping with analytical evaluation to derive practical legal and policy recommendations.

4. Results

This chapter presents the principal results derived from the descriptive and analytical examination of Metaverse technology and its implications for criminal law. The analysis yielded three principal findings. First, the Metaverse has become a distinct criminogenic environment generating four identifiable categories of offenses that existing legal frameworks do not adequately cover. Second, both substantive criminal law and procedural investigative mechanisms contain structural deficiencies that prevent effective accountability in immersive virtual spaces. Third, a pronounced regulatory divergence exists between developed jurisdictions which have begun adapting digital governance instruments and Arab legal systems, which continue to rely on general cybercrime statutes not designed for mixed-reality environments.

4.1 Nature and Scope of Metaverse-Related Crimes

The analytical review of institutional reports [5,6,8], peer-reviewed literature (Brenner, 2008; Cheong, 2022; Mackenzie, 2022) [7,9,10], and comparative legal sources identified that the Metaverse has evolved from an entertainment-based concept into a multidimensional environment integrating economic, social, and behavioural interactions. Crimes within this ecosystem were found to both resemble and transcend traditional cybercrime, distinguished by the fusion of psychological, economic, and identity-based harm in a space that blurs the boundary between the real and the virtual.

Based on this cross-source analysis, four primary categories of crime were identified:

Behavioral and interpersonal offenses, such as harassment, stalking, sexual exploitation, bullying, and virtual assault through avatars. These acts produce measurable emotional and psychological effects on victims, comparable to those experienced in physical reality.

Economic and financial crimes, including fraudulent NFT schemes, identity theft, market manipulation, and laundering of virtual assets through blockchain networks and decentralized platforms.

Intellectual-property and data-integrity violations, encompassing unauthorized duplication or modification of digital assets, avatars, or biometric identifiers.

Ideological and misinformation-based crimes, involving propaganda, radicalization, or the spread of false narratives within virtual communities.

These findings confirm that the Metaverse has become a distinct criminogenic environment requiring specific legal recognition. The inadequacy of existing frameworks is illustrated concretely by the absence of any provision within the Council of Europe's Budapest Convention on Cybercrime (2001), the primary international instrument governing cybercrime, that addresses offenses committed through avatars, virtual assets, or immersive environments. Article 2 (illegal access) and Article 3 (illegal interception) of the Convention apply only to computer systems and data, not to the experiential or identity-based harms that characterize metaverse offenses. This gap was confirmed by Interpol's Metaverse Policing Report (2023), which found that law enforcement agencies across member states consistently lacked both the legal basis and the technical capacity to investigate crimes occurring within persistent virtual environments.

4.2 General Framework of Legal Deficiencies in the Metaverse

The deficiencies identified in both substantive criminal law and procedural mechanisms stem from a shared structural challenge: the emergence of immersive virtual environments that were not contemplated by traditional legal frameworks. While substantive law struggles to define conduct, harm, and responsibility in virtual space, procedural law faces parallel difficulties in evidence collection, jurisdiction, and enforcement. For analytical clarity, these deficiencies are examined separately in Sections 4.2.1 and 4.2.2

4.2.1 Deficiencies in Substantive Criminal Law

A key result of the analysis is that current penal codes are inadequate for defining and prosecuting crimes committed in virtual environments. Most national legal systems continue to rely on traditional understandings of the criminal act, place, and result; each of which supposes physical reality.

This structural limitation has produced three core deficiencies, each demonstrable through examination of existing legal instruments:

Legislative ambiguity: Most penal codes define criminal harm by reference to physical injury or tangible property damage. For example, Article 1 of Kuwait's Law No. 63 of 2015 on Combating Information Technology Crimes defines punishable acts in terms of unauthorized access to information systems, a definition that does not extend to harassment, assault, or exploitation conducted through avatars within a shared virtual environment. Similarly, the United States Computer Fraud and Abuse Act (18 U.S.C. § 1030) criminalizes unauthorized access to "protected computers" but contains no provision covering identity-based harm or psychological injury inflicted through virtual embodiment.

Unequal protection: The EU's General Data Protection Regulation (GDPR,

Regulation 2016/679) offers the most developed framework for digital identity protection, recognizing biometric data and online identifiers as personal data under Article 4(1). However, GDPR is a data-protection instrument, not a criminal law framework. It creates civil remedies and administrative sanctions under Article 82 and Article 83, but does not criminalize the misuse of avatar identities or the infliction of psychological harm in virtual environments. Victims of avatar-based abuse therefore lack a criminal law remedy even within the most advanced regulatory jurisdiction in the world.

Doctrinal inconsistency: The absence of statutory definitions for virtual acts forces courts to apply analogical reasoning with unpredictable results. In *State v. Drew* (United States, 2009), a federal court struggled to apply the Computer Fraud and Abuse Act to a case of online harassment that caused psychological harm, ultimately rejecting the prosecution's theory due to the statute's physical-access orientation. This illustrates how doctrinal frameworks built around tangible harm cannot reliably capture the experiential injuries inflicted in immersive digital environments.

The results demonstrate that, globally and regionally, no comprehensive legal system currently provides definitions or classifications for acts that occur exclusively in immersive environments. The absence of such provisions confirms that criminal law remains tied to the material world, leaving the Metaverse largely unregulated in terms of liability and punishment.

4.2.2 Deficiencies in Procedural and Investigative Mechanisms

The procedural dimension of the paper reveals an even wider gap between emerging technology and criminal justice capacity. Evidence within the Metaverse is dynamic, intangible, and easily altered, posing significant difficulties for traditional investigative methods that rely on fixed data or physical possession.

The main procedural deficiencies identified are:

Ephemeral evidence: criminal conduct within the Metaverse often takes place through temporary audiovisual interactions or code-based events that vanish once a session ends.

Jurisdictional complexity: acts committed in the Metaverse simultaneously cross multiple national borders, involving offenders, victims, and servers located in different territories.

Institutional incapacity: police and judicial authorities lack specialized units capable of capturing, preserving, and analyzing three-dimensional or blockchain-based evidence.

Limited international cooperation: there is no harmonized framework for exchanging digital evidence or mutual legal assistance in virtual-reality crimes.

These findings establish that procedural law is structurally unprepared to confront the investigative realities of the Metaverse. The Council of Europe's Convention on Cybercrime (Budapest Convention, 2001) provides in Articles 16 and 17 for expedited preservation and partial disclosure of computer data, and Article 18 authorizes production orders for subscriber information. However, these provisions presuppose that evidence exists in a fixed, server-stored form and that a responsible service provider can be identified and compelled to produce it. Neither condition reliably holds within decentralized metaverse platforms operating on blockchain architecture, where data is distributed across nodes, session records are not retained by any single operator, and no jurisdiction has enacted rules governing the preservation of three-dimensional interaction logs or blockchain-verified event records as admissible evidence. Without such standardized rules for authentication,

preservation, and admissibility, effective prosecution remains structurally impossible rather than merely difficult.

4.3 The Debate on Electronic Legal Personality in the Metaverse

The paper's analysis demonstrates that avatars, the digital extensions of users, possess attributes of legal identity that cannot be ignored. They represent individuals' actions, carry economic value, and may become the direct subjects or objects of harm. The findings support the recognition of electronic legal personality as an emerging necessity for legal certainty in virtual environments.

If avatars and other digital entities are acknowledged as data-based legal subjects, acts such as impersonation, deletion, or unauthorized transfer of avatars could be treated as violations of personal rights or data integrity. Such recognition would align criminal law with the realities of human participation in virtual spaces, where individuals exist and act through electronic representation.

The results further indicate that a dual structure of accountability, combining human responsibility with digital personhood, offers the most coherent model for assigning liability in environments where human action and technological agency intersect.

No official authority has formally recognized electronic personality for avatars or metaverse entities. The closest analogue in positive law is the European Parliament Resolution of 16 February 2017 on Civil Law Rules on Robotics (2015/2103(INL)), which invited the European Commission to consider creating a specific legal status of "electronic persons" for sophisticated autonomous robots, defined as entities capable of making autonomous decisions or independently interacting with third parties. The Resolution explicitly proposed that such entities could hold rights, bear obligations, and be subject to liability. However, the European Commission declined to adopt this proposal, and no binding legislative instrument has since been enacted. The 2017 Resolution therefore marks the outer boundary of current legal recognition: the concept of digital personhood has been formally debated at the highest legislative level but has not been translated into enforceable law, leaving avatars and AI-driven metaverse agents in a legal vacuum.

4.4 Emergence of Financial Crime: Documented Risks and Regulatory Gaps

The research revealed that the Metaverse's economy, driven by blockchain, cryptocurrencies, and non-fungible tokens, operates largely outside traditional state supervision. This decentralization facilitates fraudulent activity, speculative manipulation, and illicit financial transfers. Evidence gathered from global financial-crime data and comparative legal studies shows that:

Decentralized transactions enable money laundering and concealment of criminal proceeds. The Financial Action Task Force (FATF) Guidance on Virtual Assets and Virtual Asset Service Providers (2022) explicitly identifies decentralized finance (DeFi) protocols and peer-to-peer virtual asset transfers as high-risk channels for money laundering. FATF's Recommendation 15 requires member states to apply anti-money-laundering obligations to virtual asset service providers (VASPs), yet the Guidance acknowledges that fully decentralized platforms without an identifiable controlling party fall outside this framework, leaving a structural regulatory gap that metaverse-based financial crime directly exploits.

"Wash trading" and artificial inflation of NFT assets constitute documented, under-prosecuted fraud. Chainalysis (2023) reported that NFT wash trading, the practice of repeatedly selling an asset between wallets controlled by the same

actor to create artificial price history, generated over USD 44 million in artificially inflated proceeds during 2022 alone. Despite constituting market manipulation under securities legislation in most jurisdictions (e.g., Section 9(a)(2) of the US Securities Exchange Act of 1934; Article 12 of the EU Market Abuse Regulation 596/2014), NFTs are not uniformly classified as securities, meaning this conduct frequently falls outside the jurisdictional reach of financial regulators entirely.

Lack of global coordination creates exploitable jurisdictional blind spots. The EU's Markets in Crypto-Assets Regulation (MiCA, Regulation 2023/1114), which entered into force in June 2023, establishes the most comprehensive regulatory framework for crypto-asset service providers to date, requiring authorization, disclosure, and AML compliance. However, MiCA applies only within the European Economic Area. Metaverse platforms operating from non-MiCA jurisdictions, or from no fixed jurisdiction at all, are not subject to its obligations, confirming that the absence of a harmonized international instrument allows actors to structure operations specifically to avoid the most stringent regulatory regimes.

The findings emphasize that the Metaverse functions as both a commercial and a criminal marketplace, where digital anonymity and asset fluidity invite exploitation. Addressing this requires new anti-money-laundering mechanisms, digital-asset transparency laws, and mandatory disclosure systems adapted to virtual economies.

4.5 The Ethical–Regulatory Gap in the Metaverse

The results also reveal a persistent ethical and legislative lag between technological innovation and regulatory response. The speed of Metaverse development has far outpaced the creation of ethical standards and legal safeguards. Governments and institutions have yet to define the boundaries of consent, data ownership, privacy, and psychological protection within immersive environments.

This gap has allowed large technology companies to dominate regulatory interpretation, designing ecosystems with minimal accountability. The absence of proactive legislation has led to moral and psychological harms, such as emotional trauma from avatar abuse or exposure to extremist content that remain beyond criminal sanction. This gap is concretely illustrated by the documented incident of avatar sexual assault within Meta's Horizon Worlds platform in 2021, in which a user reported being groped by a stranger's avatar in a virtual social space. The incident was widely reported and prompted Meta to introduce a "Personal Boundary" technical feature as its sole response. No criminal investigation was opened, no existing statutory provision in any jurisdiction was found to cover the conduct, and no platform liability was established under applicable law. Under the EU's Digital Services Act (Regulation 2022/2065), very large online platforms are required to assess and mitigate systemic risks, including risks to fundamental rights (Article 34). However, the DSA does not criminalize harmful conduct occurring on platforms, nor does it create a private right of action for victims of avatar-based abuse. The incident therefore illustrates both the legislative vacuum and the systemic reliance on self-regulatory technical measures in the absence of enforceable criminal law standards.

The paper concludes that the lag between law and technology threatens the principle of legal predictability, undermining public trust in justice systems and enabling the normalization of unregulated conduct in digital life.

4.6 Divergent Regulatory Approaches to the Metaverse

The comparative analysis revealed marked disparities between regions. Developed jurisdictions, such as the European Union, Japan, and South Korea, have

begun introducing data-protection, digital-asset, and online-safety frameworks that indirectly apply to the Metaverse. In contrast, Arab legal systems remain governed by general cybercrime laws that do not account for immersive realities.

These results demonstrate that regional fragmentation weakens international efforts to combat transnational virtual crime. The lack of harmonized legal concepts, such as digital identity, electronic personhood, and place of virtual harm, result in legal uncertainty and prevents coordinated enforcement. The paper concludes that regional legislative harmonization, especially within the Arab world, is necessary to maintain both sovereignty and legal relevance in a rapidly digitizing world.

This divergence is not merely legislative but also conceptual. The EU's Digital Services Act (DSA, Regulation 2022/2065) imposes obligations on very large online platforms, including risk assessment (Article 34), independent auditing (Article 37), and transparency reporting, that would, if applied to metaverse operators, provide a structural accountability layer currently absent elsewhere. The EU's Markets in Crypto-Assets Regulation (MiCAR, 2023/1114) further requires crypto-asset service providers to hold authorization, maintain capital requirements, and comply with AML rules under Articles 59–76. By contrast, Kuwait's Law No. 63 of 2015, Saudi Arabia's Anti-Cybercrime Law of 2007 (Royal Decree M/17), and the UAE's Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrime all define criminal acts by reference to information system access, data interference, and content-based offenses such as defamation or incitement. None contains provisions addressing virtual presence, avatar-mediated harm, digital asset fraud within immersive environments, or the forensic preservation of three-dimensional interaction evidence. The enforcement gap is therefore not merely a matter of regulatory intensity but of fundamental definitional incompatibility between what these laws cover and what metaverse crimes actually involve.

4.7 Overall Assessment

The cumulative results confirm that criminal law, both in substance and in procedure, has not yet evolved to address the realities of crime within the Metaverse. The system's conceptual foundation remains tied to physical space and tangible harm, while human behavior increasingly migrates toward digital existence.

The findings demonstrate a widening gap between technological development and legal adaptation, producing three fundamental consequences:

1. The rise of a new category of crime that escapes existing definitions and sanctions.
2. The emergence of digital harm that lacks legal recognition or remedy.
3. The erosion of jurisdictional authority in a borderless, decentralized virtual sphere.

Taken together, these results underscore the necessity for an international legal framework capable of recognizing digital personhood, defining virtual criminal acts, standardizing digital evidence procedures, and embedding ethical accountability into technological design.

5. Discussion

The results presented in Section 4 establish that criminal law, both substantive and procedural is structurally unprepared for the realities of the Metaverse. The identification of four distinct crime categories (Section 4.1), the mapping of substantive and procedural deficiencies (Section 4.2), and the comparative divergence between legal systems (Section 4.6) collectively confirm that existing frameworks

were designed for a physical world and cannot be extended to immersive virtual environments without deliberate legislative reconstruction. This discussion interprets those findings by examining their theoretical implications, identifying the underlying causes of each gap, and proposing directions for reform. The emergence of the Metaverse constitutes one of the most significant conceptual challenges to criminal law since the digital revolution, not merely a new platform for interaction, but a distinct social order where conduct, communication, and economic exchange occur through digital proxies. This hybridization demands a rethinking of fundamental doctrines: "actus reus," "mens rea," jurisdiction, and punishment.

While the Internet created a "cyberspace" where crime could occur across borders, the Metaverse adds an experiential dimension, users do not merely communicate or transact online, they inhabit a parallel world through avatars capable of sensation, emotion, and identity projection. This development has led scholars to describe it as the rise of "technosocial reality" (Floridi, 2022) [12], a domain that merges human cognition and digital code into a continuous sphere of existence. In this context, the traditional binaries of real versus virtual, physical versus digital, and act versus intent lose their clarity. Criminal law, structured around tangible acts, must now address harm that is both symbolic and experiential.

5.1 Incompatibility of Traditional Criminal Law with Virtual Conduct

The result documented in Section 4.2.1, that no legal system currently provides statutory definitions for acts occurring exclusively in immersive environments, reflects a deeper doctrinal problem: the inability of existing criminal frameworks to recognize acts committed through virtual representations.

In classical doctrines, the offense requires a physical act causing a tangible result. Yet in the Metaverse, offenses occur through avatars or data streams, producing psychological and social consequences without material contact. Research by Brenner (2008) [7] first identified this paradox as "fantasy crime," where actions in simulated environments produce real psychological harm.

Virtual harassment, incitement, or defamation cannot be dismissed as mere "play." The immersive and affective design of the Metaverse generates authentic experiences, so an avatar's assault or humiliation can evoke trauma equivalent to real-world abuse. Empirical studies on cyber-victimization (Fox & Tang, 2017 [13]; Kowalski et al., 2021 [14]) demonstrate that the emotional distress from digital harassment is comparable to physical forms of violence. Therefore, it is both ethically and legally inconsistent to exclude such conduct from the scope of criminal protection.

Legal systems must evolve toward what Sugiura (2022) [15] calls a "harm-based digital jurisprudence" – a framework that evaluates criminality according to the harm caused, not the medium through which it occurs. This means that psychological and reputational harms within immersive virtual environments should be legally cognizable injuries, subject to the same principles of accountability as traditional offenses.

5.2 Identification of Offenders and Jurisdictional Ambiguity

The decentralized, borderless nature of the Metaverse has compromised the principle of territorial jurisdiction that anchors national criminal systems. Offenders can operate from one country through avatars hosted on servers in another while harming victims located across continents. This dislocation of identity and location makes traditional mechanisms of transfer and prosecution ineffective.

Comparative legal analyses confirm this difficulty. The European Union Agency for Cybersecurity (ENISA, 2022) [8] and INTERPOL (2023) [6] both report that transnational cyber investigations face obstacles of data sovereignty, privacy regulations, and conflicting procedural laws. The Budapest Convention on Cybercrime (2001) offers partial solutions, but it remains state-centric and technologically outdated. Scholars such as Clough (2020) [16] and Broadhurst (2021)[17] advocate for a new Digital Jurisdiction Treaty, which would allow nations to share evidentiary data and prosecute offenses committed within decentralized digital ecosystems.

Moreover, the rise of blockchain-based identity systems and decentralized autonomous organizations (DAOs) introduces actors that are not natural persons but algorithmic collectives. Assigning liability in such contexts challenges the anthropocentric assumptions of criminal law. The notion of meta jurisdiction, a legal regime operating simultaneously across real and virtual domains, foreshadows what global governance must eventually become; a coordinated digital legal order recognizing the simultaneity of actions across multiple realities.

5.3 The Legal Status of Avatars and the Question of Electronic Legal Personality

Avatars, as digital embodiments of individuals, complicate the definition of legal personhood. Under current frameworks, they are treated as software interfaces or property, not as subjects of rights. Yet their function in the Metaverse blurs this line. They express will, perform labor, own property, and interact autonomously through AI assistance. Which is why the recognition of electronic legal personality, granting avatars limited legal standing as extensions of human identity is crucial.

This proposition aligns with emerging European discourse on e-personhood, debated within the European Parliament since 2017 regarding autonomous robotics (European Commission, 2017) [18]. Scholars such as Gless, Silverman, and Weigend (2016) [19] argue that recognizing limited personhood for artificial agents would clarify accountability and prevent impunity. Conversely, opponents like Bryson (2019)[20] caution that attributing personhood to non-human entities may dilute human responsibility.

A balanced solution, supported by Edwards and Veale (2023) [21], lies in hybrid accountability, where the natural user retains ultimate responsibility, but avatars hold derivative procedural rights (e.g., restitution for destruction or impersonation). Recognizing such status would allow law to mirror the evolving philosophy of digital identity, neither entirely fictional nor fully autonomous but juridically real.

5.4 Financial Crimes and Market Manipulation in the Virtual Economy

The economic architecture of the Metaverse, built on cryptocurrencies, non-fungible tokens (NFTs), and decentralized finance (DeFi), present vast criminogenic potential. Transactions occur anonymously and globally, often beyond the oversight of central banks. With money laundering, fraud, and speculative manipulation being the primary threats to virtual financial integrity.

Empirical research supports these concerns. Chainalysis (2023) [22] reported that NFT wash trading accounted for over USD 1.3 billion in illicit gains during 2022. The anonymity of digital wallets allows the concealment of criminal proceeds, frustrating enforcement of anti-money-laundering (AML) laws. The Financial Action Task Force (FATF, 2022) [23] warns that virtual asset service providers (VASPs) remain the weakest link in global AML compliance.

Legal scholars such as Houben and Snyers (2018) [24] and McGinnis (2021)[25] argue that blockchain's immutability can be turned into an evidentiary advantage

if regulators enforce “traceable transparency.” Calling for mandatory integration of blockchain-verified audit trails into Metaverse platforms. Such protocols would balance user privacy with the necessity of criminal accountability.

Without comprehensive regulation, the Metaverse risks replicating the structural failures that enabled financial crimes during the early Internet era, only now amplified by automation, global scale, and algorithmic speed.

5.5 Challenges in Law Enforcement and Digital Evidence Collection

Law enforcement agencies are currently ill-equipped to operate within virtual environments. Evidence in the Metaverse is dynamic, encrypted, and often ephemeral, manifesting as gestures, voice interactions, or 3D simulations. Conventional forensic methods cannot capture these experiences without disrupting user privacy or platform integrity.

To overcome this challenge, the creation of Metaverse-specific procedural law that define the standards for evidence preservation, avatar interrogation, and cross-border data access is vital. This vision parallels the recommendations of INTERPOL’s Metaverse Policing Report (2023) [6], which advocates for digital chain-of-custody protocols, avatar-based police agents, and blockchain authentication of evidence.

Recent academic models by Casey and Turnbull (2022) [26] suggest the use of forensic virtualization, in which law enforcement recreates digital scenes using metadata to reconstruct events. However, these methods raise privacy concerns and require strong judicial oversight. Establishing an international Digital Evidence Charter, a codified framework for admissibility and verification, would ensure procedural fairness across jurisdictions.

5.6 Ethical and Legislative Lag Behind Technological Advancement

A recurring theme is the chronological dislocation between innovation and legislation. Technological progress moves exponentially, whereas law evolves linearly. As a result, legislators react only after harm has occurred. Floridi (2022) [12] calls this the “ethical lag” of the digital age: a failure of governance imagination.

Corporations developing Metaverse technologies have exploited this vacuum, deploying immersive systems with little ethical oversight. Issues such as consent in virtual interaction, psychological safety, and biometric surveillance remain under-regulated. Studies by Madary and Metzinger (2016) [27] and Bublit (2020) [28] demonstrate that extended exposure to virtual environments can alter cognition and emotional regulation, raising the possibility of psychological harm independent of criminal intent.

This paper advocates for anticipatory regulation, embedding ethical safeguards within technological design, an approach also supported by Susskind (2022) [29], who proposes “law by architecture,” meaning legal norms encoded directly into system infrastructure. Legislators must thus move from reactive punishment to proactive governance, ensuring that innovation does not precede moral accountability.

5.7 The Arab Legal Context and the Imperative for Reform

Within the Arab region, criminal legislation has not yet adapted to the challenges of virtual crime. Current cybercrime laws, such as Kuwait’s Law No. 63 of 2015, Saudi Arabia’s Anti-Cybercrime Law (2007), and the UAE’s Cybercrime Decree (2021), focus primarily on data breaches, hacking, and online defamation. None explicitly address crimes in mixed-reality environments.

This paper underscores the necessity of comprehensive legislative reform. Arab states should integrate Metaverse-specific provisions into penal codes, redefining

“location of crime,” “digital identity,” and “means of commission.” Establishing regional coordination through the Arab League’s Cybercrime Convention, currently under review, which could possibly harmonize procedures and evidence standards.

Comparative analysis with the European Digital Services Act (2022) demonstrates that proactive regional frameworks enhance resilience against cyber threats. Furthermore, adopting Arab-centric ethical guidelines rooted in Sharia’s principles of justice and prevention could create a culturally consistent model of virtual governance, balancing modernization with moral tradition.

5.8 Toward a New Philosophy of Criminal Justice in the Virtual Age

Ultimately, the Metaverse exposes the inadequacy of a purely materialistic conception of law. Justice must now extend beyond protecting bodies and property to safeguarding digital identity, cognitive autonomy, and virtual dignity. Rather than abandoning spatial considerations altogether, contemporary criminal justice increasingly extends its protective scope beyond purely physical space to address harms affecting identity, dignity, and psychological integrity within hybrid virtual environments.

This paper calls for a reconstruction of criminal philosophy, one that recognizes harm as both physical and symbolic, crime as both action and algorithm, and justice as both territorial and trans-reality. This approach aligns with the emerging field of techno-legal criminology (Yar, 2020) [30], which studies how social control operates across cyber-physical systems.

The future of law will depend on the capacity to integrate technology without surrendering humanity. As Heller (2023) [31] observes, the Metaverse can either expand freedom or amplify control; the outcome depends on how justice is encoded into its infrastructure. Criminal law, therefore, must evolve from static codification to dynamic adaptation, anchored in human dignity, yet capable of navigating the fluidity of digital life.

6. Conclusion

The Metaverse represents both an extraordinary human achievement and a profound challenge to the limits of legal thought. What began as a technological vision has evolved into a tangible social and economic realm, revealing the deep shortcomings of traditional criminal law in addressing conduct that transcends physical boundaries. Through this research, we demonstrated how crimes emerging within this environment – whether psychological, financial, or identity-based – demand a new legal consciousness capable of bridging the divide between the virtual and the real. Unless the law advances with equal speed and foresight, the distance between innovation and accountability will continue to expand, weakening the very foundations of justice. The path forward requires embracing digital personhood, standardizing evidentiary mechanisms, and adopting anticipatory frameworks that embed ethics and responsibility within technological design. Only then can criminal law reclaim its essential purpose: to safeguard human dignity in every dimension of existence – real or virtual.

6.1 Practical implications

Legislators should: (i) adopt statutory definitions for digital identity, virtual assets, and immersive harms; (ii) recognize identity-based and psychological harms in immersive environments as legally cognizable interests; (iii) modernize jurisdictional rules to address multi-location crimes involving users, servers, and platforms across

borders; and (iv) establish procedural standards for capturing, preserving, and authenticating immersive digital evidence. Internationally, harmonized mutual legal assistance mechanisms and cross-border evidence-sharing protocols are essential to prevent jurisdictional safe havens.

6.2 Future empirical research

Future research should incorporate empirical case studies drawn from real incidents such as avater-based harassment, NFT-related fraud, and cross-platform identity impersonation to test the effectiveness of emerging regulatory and enforcement approaches.

Author contributions: Conceptualization, AA and MA; methodology, AA and MA; formal analysis, AA and MA; investigation, AA and MA; resources, AA and MA; writing – original draft preparation, AA; writing – review and editing, MA; supervision, MA; project administration, AA. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflict of interest: The authors declare that they have no conflicts of interest regarding the publication of this paper.

References

1. United Nations Economic and Social Commission for Western Asia (ESCWA). The Metaverse and the Future of the Arab Region: Choices and Actions. 2024. Available online: <https://www.unescwa.org/publications/metaverse-arab-region-future-choices-actions> (accessed on 5 April 2026).
2. Zidan AM, Al-Suwaidi S. The world beyond the traditional: Metaverse. 2022. Available online: https://www.researchgate.net/publication/372166277_The_world_beyond_the_traditional_Metaverse (accessed on 5 April 2026).
3. Al-Sisi SH. The virtual world and the real world: A vision for technological and cognitive hegemony. 2022. (accessed on 5 April 2026).
4. Ibrahim KM. Legal regulation of metaverse technology. 2023. Available online: https://mjle.journals.ekb.eg/article_320323.html?lang=en (accessed on 5 April 2026).
5. Elliptic. The future of financial crime in the metaverse: Fighting crypto-crime in Web 3.0. Elliptic; 2022. Available online: <https://www.elliptic.co/resources/crime-in-the-metaverse> (accessed on 5 April 2026).
6. INTERPOL. Metaverse policing and investigative readiness report. International Criminal Police Organization; 2023. Available online: <https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf> (accessed on 5 April 2026).
7. Brenner SW. Fantasy crime: The role of criminal law in virtual worlds. *Vanderbilt Journal of Entertainment & Technology Law*. 2008, 11(1): 1–57. Available online: <https://scholarship.law.vanderbilt.edu/jetlaw/vol11/iss1/1> (accessed on 5 April 2026).
8. ENISA. Metaverse security and legal implications report. European Union Agency for Cybersecurity; 2022. Available online: <https://www.enisa.europa.eu/publications> (accessed on 5 April 2026).
9. Cheong BC. Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity Law Review*. 2022, 3(2): 467–494. doi:10.1365/s43439-022-00071-8.
10. Mackenzie S. Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *British Journal of Criminology*. 2022, 62(6): 1537–1552. <https://doi.org/10.1093/bjc/azab118>.
11. Filipova I. Creating the metaverse: Consequences for economy, society, and law. *Digital Law Journal*. 2023, 1(1). https://www.lawjournal.digital/jour/article/view/7/pdf_4 (accessed on 5 April 2026).
12. Floridi L. *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford Academic; 2023. <https://doi.org/10.1093/oso/9780198883098.001.0001> <https://doi.org/10.1093/oso/9780198883098.001.0001> (accessed on 1 April 2026).
13. Fox J, Tang WY. Women’s experiences with general and sexual harassment in online video games: Prevalence and predictors

- of online harassment. *Journal of Interpersonal Violence*. 2017, 32(19): 2831–2854. DOI:10.1177/1461444816635778
14. Kowalski R, Limber S, Agatston P. *Cyberbullying: Bullying in the digital age*. 3rd ed. Wiley-Blackwell; 2021. Available online: <https://www.wiley.com/en-us/Cyberbullying%3A+Bullying+in+the+Digital+Age%2C+3rd+Edition-p-9781119164944> (accessed on 5 April 2026).
 15. Sugiura L. *Digital harm and responsibility: Toward a criminology of online conduct*. Policy Press; 2022. Available online: <https://policy.bristoluniversitypress.co.uk/digital-harm-and-responsibility> (accessed on 5 April 2026).
 16. Clough J. *Principles of cybercrime*. 2nd ed. Cambridge University Press; 2015. Available online: <https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718> (accessed on 5 April 2026).
 17. Broadhurst R. *Cybercrime, jurisdiction, and global governance*. Routledge; 2021. Available online: <https://www.routledge.com/Cybercrime-Jurisdiction-and-Global-Governance/Broadhurst/p/book/9780367609290> (accessed on 5 April 2026).
 18. European Parliament. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). In: *Proceedings of the European Parliament*; 16 February 2017; Brussels, Belgium. Available online: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (accessed on 5 April 2026).
 19. Gless S, Silverman E, Weigend T. If robots cause harm, who is to blame? *New Criminal Law Review*. 2016, 19(3): 412–436. <https://doi.org/10.1525/nclr.2016.19.3.412>
 20. Bryson JJ. The artificial intelligence and robot debate: Why we should not legalise autonomous machine personhood. *AI & Society*. 2019, 34(1): 49–55. <https://link.springer.com/article/10.1007/s00146-018-0820-0> (accessed on 5 April 2026).
 21. Edwards L, Veale M. *Regulating AI and automated systems*. Oxford University Press; 2023. Available online: <https://global.oup.com/academic/product/regulating-ai-and-automated-systems-9780198887515> (accessed on 5 April 2026).
 22. Chainalysis. *The 2023 Crypto Crime Report*. Chainalysis Inc.; 2023. Available online: <https://www.chainalysis.com/blog/nft-wash-trading-report-2023/>. (accessed on 1 April 2026).
 23. FATF. *Updated guidance for a risk-based approach to virtual assets and VASPs*. Financial Action Task Force; 2022. Available online: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> (accessed on 5 April 2026).
 24. Houben R, Snyers A. *Cryptocurrencies and blockchain: Legal context and implications for financial crime*. European Parliament Research Service; 2018. Available online: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282018%29619024 (accessed on 5 April 2026).
 25. McGinnis J. Blockchain transparency and regulatory enforcement. *Harvard Business Law Review*. 2021, 11(2): 187–220. Available online: <https://www.hblr.org/2021/blockchain-transparency-and-regulatory-enforcement/> (accessed on 1 April 2026).
 26. Casey E, Turnbull B. Forensic virtualization: Reconstructing digital events in immersive environments. *Forensic Science International: Digital Investigation*. 2022, 40: 301317. Available online: <https://www.sciencedirect.com/science/article/pii/S2666281721002687> (accessed on 1 April 2026).
 27. Madary M, Metzinger T. Real virtuality: A code of ethical conduct. Recommendations for good scientific practice and the consumers of VR-technology. *Frontiers in Robotics and AI*. 2016, 3: 3. <https://doi.org/10.3389/frobt.2016.00003>.
 28. Bublitz JC. Virtual violence, emotions, and the criminal law. *Criminal Law and Philosophy*. 2020, 14(2): 177–202. <https://link.springer.com/article/10.1007/s11572-019-09496-9> (accessed on 5 April 2026).
 29. Susskind R, Daniel Susskind, *The Future of the Professions: How Technology Will Transform the Work of Human Experts* (Oxford, 2015; online edn, Oxford Academic, 12 Nov. 2020), <https://doi.org/10.1093/oso/9780198713395.001.0001..>
 30. Yar, M. (2020). *Cybercrime and society* (3rd ed.). Sage Publications. Available online: <https://us.sagepub.com/en-us/nam/cybercrime-and-society/book268275> (accessed on 5 April 2026).
 31. Heller N. Law in the metaverse age: Governance, control, and autonomy. *Yale Journal of Law & Technology*. 2023, 25(2): 211–247. Available online: <https://yjolt.org/law-metaverse-age> (accessed on 10 April 2026).