VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CRIMINAL RESPONSIBILITY IN METAVERSE: COMPARATIVE ANALYSIS OF THE U.S., EU, AND INDIA

- Bhavya Sharma & Akanksha Sharma[1]

ABSTRACT

The emergence of the metaverse, a persistent, immersive virtual environment where users engage through avatars in augmented or virtual reality settings, has opened up new avenues for social interaction, trade, human activity, and regrettably, criminal conduct. Although many countries rely on conventional criminal law frameworks that were created for physical spaces, these frameworks might not be adequate to deal with crimes committed in virtual worlds.

This article explores how acts such as harassment, assault, theft of virtual assets, and identity fraud manifest in the metaverse, and compares how the United States, the European Union, and India currently approach liability, jurisdiction, and enforcement. It argues that the core criminal law concepts of actus reus, mens rea, and legal harm must be re conceptualised for immersive virtual environments.

In order to prevent the metaverse from turning into a lawless area of actual harm, the article suggests a hybrid architecture that combines modified national criminal laws, platform governance procedures, and international cooperation.

KEYWORDS: Metaverse, Metacrime, Virtual Crimes, Criminal Laws, Avatar liability.

INTRODUCTION

The concept of the metaverse has evolved rapidly from speculative fiction into a tangible, expansive virtual environment in which users—represented by avatars—live, work, socialise

[1] Guru Nanak Dev University, Amritsar

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

and transact. In these contexts, immersive technologies like virtual reality (VR), augmented reality (AR), and blockchain-based digital assets come together to create persistent worlds that represent many aspects of the "real" world but are not limited by geography, physical embodiment, or temporal boundaries.

The question of whether injuries sustained and committed in the metaverse should be covered by criminal law? For example, if an avatar is virtually sexually assaulted, or virtual goods of real economic value are stolen, or if an avatar is harassed to the point of psychological trauma, does the existing criminal law suffice? This article argues that the unique characteristics of the metaverse—avatar-mediated embodiment, durable virtual property, cross-border platforms, and the blurring of virtual and real harm—make the current criminal law frameworks in these jurisdictions increasingly insufficient. It contends that a hybrid framework that combines national law, platform governance, and international cooperation is the best course of action and that we must rethink the fundamental concepts of actus reus, mens rea, legal injury, and jurisdiction in this new context.

UNDERSTANDING METAVERSE AND METACRIMES

The metaverse, a term coined by Neal Stephenson in his 1992 novel Snow Crash, has evolved from a science fiction concept to a tangible digital ecosystem where users interact through avatars in immersive virtual environments.[2]Facilitated by virtual reality (VR), augmented reality (AR), and blockchain technologies, the metaverse offers a parallel universe for socialization, commerce, and entertainment.[3] The “metaverse” remains a loosely defined concept, but it is commonly understood as a persistent, shared virtual 3D environment combining VR/AR, digital assets, avatars and immersive interaction.[4]

However, this digital frontier has also become a breeding ground for novel criminal activities, collectively termed "metacrime," which include virtual sexual assault, financial fraud, and

[2] Neal Stephenson, Snow Crash (Penguin, 1992).
[3] GD Ritterbusch and MR Teichmann, ‘Defining the Metaverse: A Systematic Literature Review’ (2023) 11 IEEE Access 12368.
[4] Kasiyanto & Kilinc, The Legal Conundrums of the Metaverse, 1 J. Cent. Banking L. & Insts. 299, 299–322 (2022). jcli-bi.org

identity theft.[5] Therefore, in considering virtual crime, it is useful to identify different categories of offending behaviour in the metaverse: (i) personal offences (e.g., harassment, virtual assault), (ii) property/economic offences (e.g., theft of digital assets), and (iii) identity/fraud offences (e.g., avatar impersonation, deep-fakes). Unlike traditional online misconduct, these acts occur in immersive, interactive spaces where users experience a heightened sense of presence, making the psychological and economic impact more tangible. For instance, a virtual assault in a VR environment may have no physical contact but can cause severe emotional distress, raising questions about whether existing laws should recognize such harm as equivalent to physical assault.

According to comparative research, "virtual crimes" should be given particular consideration because they can cause actual harm despite lacking physical components: "The criminal metaverse... may include atypical offences that, while lacking physical harm, could activate the nervous system much like a conventional crime."[6] This finding emphasizes the necessity of reexamining the harm principle of criminal law in the metaverse.

Applying Criminal Law Principles to Virtual Conduct:

(A) Actus Reus

In traditional criminal law, liability arises from a voluntary act (or a culpable omission) that causes harm. In virtual environments such as the metaverse, this “act” is carried out through an avatar rather than a physical body. The question then becomes whether an avatar’s movement can be treated as the user’s own actus reus. Some legal systems may regard the avatar’s actions as an extension of the user’s physical intent, but this link is not always clear. Technical problems—like system glitches, latency issues, or external hacking—can disrupt user control, creating uncertainty about whether the act was voluntary in the legal sense.

(B) Mens Rea

Proving intent in the metaverse poses unique challenges. Anonymity, identity masking, and the blurred boundary between play and reality make it difficult to show that a user possessed

[5] GM Bovenzi, ‘MetaCrimes: Criminal Accountability for Conducts in the Metaverse’ (2023) Companion Proceedings of the ACM Web Conference 565.

[6] Eldar Haber, *The Criminal Metaverse*, 99 Ind. L.J. ___ (2024). repository.law.indiana.edu

criminal intent. A defendant may argue that they perceived the conduct as part of a game, not as a real-world offence. Scholars have noted that when users interact through avatars, it becomes harder to establish the subjective mental element required for crimes such as assault, harassment, or fraud.

(C) The Harm Principle

Traditional criminal law relies on tangible harm—physical injury, property damage, or direct moral wrongdoing. Virtual spaces complicate this model. Psychological trauma, reputational loss, and the theft or destruction of digital assets all raise questions about what qualifies as legally recognizable harm. Although the law may not yet classify the misappropriation of virtual property as "theft" in the statutory sense, the resulting economic loss and emotional distress can be genuine. Some researchers even suggest that the human nervous system responds similarly to virtual assault in immersive environments and to real-world physical attacks, indicating that such harms should not be dismissed as mere simulation.

Although they need to be reinterpreted for virtual situations, the fundamental ideas of criminal law nevertheless offer a helpful place to start. The concept of purpose needs to change to accommodate immersive and semi-anonymous environments, the avatar needs to be rethought as a possible site of action, and the concept of damage needs to change to encompass injuries that happen digitally but have actual psychological or financial effects.

LEGAL GAP IN PROSECUTING METACRIMES

From a legal perspective, the metaverse poses multiple challenges. First, the borderless, persistent and interoperable nature of the space blurs the traditional territorial basis for regulatory jurisdiction.[7] Second, private platform governance (by companies such as Meta, Decentraland, Roblox, etc.) plays a dominant role in moderating behaviour and defining terms of service, rather than public criminal law.[8]Third, many acts in the metaverse (such as virtual harassment or groping of avatars) generate real psychological or economic harm, yet may lack a clear analogue in statutory criminal law.[9]

[7]INTERPOL, *Metaverse: A Law Enforcement Perspective*, at 2 (2023). Interpol
[8]Eldar Haber, *The Criminal Metaverse*, 99 Ind. L.J. ___ (2024). repository.law.indiana.edu
[9]Al Adwan & Ehjelah, Crimes Committed on Metaverse Platforms and the Challenges They Pose to Criminal Law, Dirasat: Shari'a & Law Sci. (2025). DSR

These features mean criminal law has, so far, lagged behind. According to a recent study, "traditional criminal law falls short in addressing acts committed within the metaverse" due to the difficulty of determining the subjective aspect (intent) when avatars mediate behavior and the complexity of gathering evidence in decentralized systems. Hence, there is a “legal vacuum” in which virtual crimes may evade prosecution or deterrence.

The prosecution of virtual crimes presents several challenges. Jurisdictional ambiguity is a central issue because metaverse platforms often operate globally, with participants located in multiple countries. Determining which legal system has authority over a virtual incident is complex. Evidence collection is also problematic; while virtual platforms generate digital logs and blockchain records, attributing these actions to a specific real-world individual often requires sophisticated forensic methods. Moreover, conventional criminal law primarily addresses physical or financial harm, leaving a conceptual gap when dealing with psychological injury or harm to virtual property. The legal recognition of virtual property rights further complicates matters, as assets acquired in the metaverse may have real-world value but lack clear legal status in many jurisdictions.

COMPARATIVE LEGAL APPROACHES

THE UNITED STATES

In the United States, the legal system has largely adapted existing cybercrime laws to address metaverse-related harms. The Computer Fraud and Abuse Act (CFAA) can be applied to hacking or unauthorized access of virtual platforms. The Sexual Offences Act 2003 and the Protection from Harassment Act 1997 provide limited recourse for metaverse offences. The former requires physical contact, while the latter may apply to harassment but still struggles with virtual contexts.[10]The proposed Online Safety Bill (2021) aims to regulate harmful content but lacks specificity for metaverse interactions.[11] State-level harassment and cyberstalking laws have occasionally extended to VR interactions. Property disputes involving NFTs and other digital assets are litigated under contract and property law frameworks.

[10]Protection from Harassment Act 1997, s 2 (UK).
[11] ‘Challenges in the Metaverse Jurisdiction and International Treaty Law’ (2023) IRPJ 1.

The U.S. approach is notable for its flexibility, allowing courts to apply existing statutes creatively. However, this flexibility results in inconsistent outcomes, as interpretations differ across jurisdictions. Moreover, the absence of metaverse-specific statutes leaves certain virtual misconduct—such as avatar-based assault or harassment—unregulated or under-prosecuted, but fewer jurisdictions have explicitly criminalised "avatar assault".[12]Legal scholars argue that while the U.S. system encourages technological innovation, it risks leaving victims without clear remedies due to fragmented regulatory coverage.

THE EUROPEAN UNION

The European Union adopts a more structured, rights-centered approach. Regulations like the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR) impose obligations on platform operators to moderate harmful content and protect personal data. These frameworks indirectly address metaverse-related harms, particularly concerning minors and vulnerable populations. EU member states increasingly interpret existing cybercrime laws to cover virtual harassment, identity theft, and fraud. Consumer protection laws further provide accountability mechanisms for transactions involving virtual assets.

Compared to the U.S., the EU prioritizes preventive measures and user safety. This approach reduces uncertainty but can be criticized for potentially stifling innovation due to stricter regulatory requirements. Overall, the EU model emphasizes user rights and platform responsibility, reflecting a preventive and protective stance toward digital harms.

INDIA'S EMERGING LEGAL APPROACH

India's legal approach to the metaverse is still emerging. While there are no dedicated laws for virtual crimes, authorities recognize the growing challenges posed by digital spaces. Union Home Minister Amit Shah has remarked that security threats have evolved "from

[12]Singh & Rajput, *Metaverse: Surging Need for Competent Laws with Increasing Metaverse Crimes*, 5 Int'l J. Law Mgmt & Hum at 716–17. IJLHM

dynamite to metaverse" and "hawala to crypto," signaling governmental awareness of these new risks.[13]

Existing statutes provide some tools for addressing online harms. The Information Technology Act, 2000 (IT Act) criminalizes hacking, cyber fraud, and the transmission of offensive content. The Bharatiya Nyaya Sanhita, 2023 addresses harassment, stalking, and defamation, while the Protection of Children from Sexual Offences Act, 2012 (POCSO) applies to online sexual exploitation of minors.[14] However, these laws were drafted with conventional cyberspace in mind and do not explicitly account for the immersive, avatar-based nature of metaverse interactions.

Legal scholars highlight several gaps in India's current framework. There is no statutory recognition of virtual assault, identity impersonation, or theft of blockchain-based assets. Jurisdictional issues are particularly acute in cross-border platforms. Moreover, the legal recognition of virtual property remains ambiguous, despite the real economic value of NFTs and virtual land.[15]

Despite these gaps, India is beginning to explore solutions. Draft provisions in the proposed Digital India Act suggest potential regulation of virtual crimes alongside oversight of social media and OTT platforms.[16] Policy reports recommend robust content moderation, identity verification, and possibly a dedicated "Metaverse Criminal Code" to govern avatar-based conduct. India is also engaging in international cybersecurity initiatives under the G20 framework, reflecting an awareness of the need for cross-border legal cooperation.[17]

COMPARATIVE ANALYSIS: U.S., EU and INDIA

[13] Business Standard, Security challenges have evolved from 'dynamite to metaverse': Amit Shah, (July 13, 2023), https://www.business-standard.com/india-news/security-challenges-have-evolved-from-dynamite-to-metaverse-amit-shah-123071300358_1.html.

[14] TheLeaflet, Our Legal System Is Still Not Ready to Regulate Users' Behaviour on the Metaverse (2024), https://theleaflet.in/civil-justice/our-legal-system-is-still-not-ready-to-regulate-users-behaviour-on-the-metaverse.

[15] Legal Service India, Legal and Regulatory Issues in India That Are Distinct to Metaverse, https://www.legalserviceindia.com/legal/article-10704-legal-and-regulatory-issues-and-challenges-in-india-that-are-distinct-to-metaverse.html

[16] NLS Web Primer, The Metaverse and Law (2023), https://www.nls.ac.in/wp-content/uploads/2023/03/NLS-WEB-PRIMER-2-metaverse.pdf.

[17] Economic Times, G20 nations should work together to take on cybersecurity threats from darknet, metaverse: Amit Shah, https://government.economictimes.indiatimes.com/news/secure-india/g20-nations-should-work-together-to-take-on-cybersecurity-threats-from-darknet-metaverse-amit-shah/101729480

Comparing the approaches of the U.S., EU, and India reveals distinct priorities and challenges. The U.S. emphasizes flexibility and litigation-driven remedies but suffers from jurisdictional fragmentation and uneven protection for victims. The EU adopts a preventive, rights-based model that prioritizes user safety, privacy, and accountability but risks regulatory overreach that could stifle innovation. India, in contrast, is at an early stage of legal adaptation, heavily reliant on existing cybercrime statutes but increasingly aware of the need for specialized frameworks.

This comparative analysis suggests that an effective legal model for the metaverse should integrate elements from all three approaches: clear statutory definitions for virtual crimes (as in India's proposed reforms), preventive measures and user rights protections (as in the EU), and flexibility to accommodate technological innovation (as in the U.S.). Such a hybrid framework would provide clarity, promote safety, and enable cross-border cooperation.

POLICY RECOMMENDATIONS

To address the challenges of metaverse crimes, several measures are necessary. First, legislatures must codify virtual assaults, harassment, fraud, and property theft to provide clear legal definitions and deterrents. Existing criminal laws can be adapted by redefining elements like "harm" and "contact" to include virtual interactions. For instance, the UK could amend the Sexual Offences Act to recognize avatar-based assaults as offences, focusing on psychological harm rather than physicality.[18]

Second, international frameworks should clarify jurisdictional responsibilities, given the global nature of metaverse platforms. A unified international legal framework is essential to address jurisdictional conflicts. A proposed Metaverse Model Criminal Code could define offences, penalties, and avatar accountability, drawing on Sweden's sexual molestation laws that prioritize "sexual integrity" over physical harm.[19]

Third, forensic standards need to evolve to attribute virtual actions to real-world actors, using blockchain analysis, VR logs, and other digital evidence. Technological solutions, like AI-

[18] 'From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse' (2025) Oxford Journal of Legal Studies.
[19] Swedish Criminal Code, Chapter 6, s 7.

driven content moderation and forensic tools for evidence collection, could enhance policing capabilities.[20]

Fourth, platform liability should be clearly defined, balancing user protection with innovation and privacy concerns. Platforms should also implement mandatory avatar registration to reduce anonymity and ensure accountability.[21]

Finally, public awareness campaigns should emphasize that actions in virtual environments can carry real-world legal consequences, bridging the perception gap between virtual and physical harm.

CONCLUSION

The metaverse presents novel challenges for criminal law, blurring the line between virtual and real-world consequences. Countries such as the U.S. and the EU have begun adapting existing legal frameworks to address these emerging issues, while India is beginning to recognize the scope and risks of virtual crimes but lacks a comprehensive statutory approach. Moving forward, legislative clarity, technological innovation in digital forensics, cross-border cooperation, and user education will be essential to protect individuals and hold perpetrators accountable. A hybrid legal framework, informed by international best practices and tailored to local realities, offers the most promising approach to safeguarding users and ensuring justice in this immersive digital domain. Ultimately, the law must evolve not merely to punish virtual misconduct but to preserve safety, trust, and fairness in immersive digital worlds.

[20] 'Metaverse Policing: A Systematic Literature Review' (2023) ScienceDirect.
[21] 'Crime and Punishment in the Metaverse: A Primer' (ORF, 2 January 2024)