Virtual Crime, Real Punishment: The Legal Vacuum in Metaverse Offences

Monnaf Ali Miah

LL.B, LL.M

Department Of Law

Rajiv Gandhi University, Arunachal Pradesh, India

Abstract

The emergence of the metaverse—a digital ecosystem blending virtual and augmented realities—has introduced unprecedented opportunities for social interaction, commerce, and innovation. However, it has also given rise to novel forms of criminality, termed "metacrime," which challenge existing legal frameworks. Offences such as virtual sexual assault, identity theft, financial fraud, and harassment within the metaverse raise complex questions about jurisdiction, liability, and the applicability of traditional criminal law. This paper examines the legal vacuum surrounding metaverse offences, highlighting the inadequacies of current laws in addressing virtual harms that produce real-world psychological and economic impacts. Through a doctrinal and comparative analysis, it explores jurisdictional challenges, the absence of corporeal elements in virtual crimes, and the difficulties in attributing liability to avatars. The paper proposes a hybrid legal framework combining adapted national laws, international cooperation, and industry self-regulation to address metacrime effectively. It argues for the recognition of avatars as extensions of legal personality and the development of metaverse-specific regulations to ensure user safety and accountability.

Keywords: Metaverse, Metacrime, Virtual Crime, Cyberlaw, Jurisdiction, Avatar Liability, Sexual Violence, Legal Framework, Data Protection, International Law

1. Introduction:

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.[1] Facilitated by virtual reality (VR), augmented reality (AR), and blockchain technologies, the metaverse offers a parallel universe for socialization, commerce, and entertainment.[2] 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 identity theft.[3] These

offences, while occurring in virtual spaces, often result in real-world psychological, emotional, and economic harm, raising urgent questions about legal accountability and punishment.

The legal vacuum in addressing metaverse offences stems from the inadequacy of traditional criminal law, which relies on physicality and territoriality, to regulate a decentralized, borderless digital realm. For instance, a 2024 case in the UK involving the virtual gang rape of a minor's avatar highlighted the psychological trauma akin to physical assault, yet existing laws struggled to categorize the offence.[4] This paper argues that the absence of a robust legal framework for metaverse offences undermines user safety and perpetuates a culture of impunity in virtual spaces. Through a doctrinal and comparative analysis, it examines the challenges of jurisdiction, the lack of corporeal elements, and avatar liability, proposing a hybrid legal model to bridge the gap between virtual crime and real punishment.

2. Understanding the Metaverse and Metacrime:

2.1 Defining the Metaverse

The metaverse is a decentralized, interoperable, and immersive 3D online environment that persists beyond individual user sessions, enabling interactions via avatars.[5] Unlike traditional cyberspace, the metaverse integrates VR, AR, and blockchain technologies to create a seamless blend of physical and digital realities.[6] Companies like Meta, Microsoft, and Roblox have invested billions to develop platforms where users can work, socialize, and transact using cryptocurrencies and non-fungible tokens (NFTs).[7] This convergence of technologies amplifies the potential for both legitimate and illicit activities.

2.2 The Nature of Metacrime

Metacrime encompasses a range of offences unique to the metaverse, including virtual sexual assault, financial fraud, identity theft, and harassment.[8] Unlike traditional cybercrime, metacrime leverages the immersive nature of the metaverse, where haptic devices and advanced avatars enhance sensory experiences, making virtual harms feel acutely real.[9] For example, the Centre for Countering Digital Hate reported that 49% of women using VR platforms experienced sexual harassment, underscoring the prevalence of gendered violence in virtual spaces.[10] INTERPOL's 2024 classification identifies ten categories of metacrime, including sexual offences, financial crimes, and acts causing emotional distress, highlighting their multidimensional nature.[11]

3. Legal Challenges in Prosecuting Metaverse Offences:

3.1 Jurisdictional Ambiguities

The borderless nature of the metaverse complicates jurisdictional authority. Traditional criminal law relies on territorial jurisdiction, where the location of the offence determines the applicable law.[12] In the metaverse, however, avatars operated by users in different countries interact in a shared digital space, raising questions about which jurisdiction governs.[13] For instance, if a user in the UK assaults an avatar

controlled by a user in South Korea, determining the locus delicti (place of the crime) becomes problematic.[14] The lack of a global regulatory authority exacerbates this issue, as existing treaties like the Budapest Convention on Cybercrime do not explicitly address metaverse-specific offences.[15]

3.2 Absence of Corporeal Elements

Traditional criminal law often requires physical elements, such as bodily harm or penetration, to constitute offences like assault or rape.[16] In the metaverse, avatars lack physical bodies, rendering laws like the UK's Sexual Offences Act 2003 inapplicable in their literal sense.[17] For example, a virtual sexual assault case reported in 2024 could not be prosecuted under existing UK laws due to the absence of physical contact, despite the victim's psychological trauma.[18] This disconnect between virtual acts and real-world harm necessitates a redefinition of criminal elements to include digital interactions.

3.3 Avatar Liability and Anonymity

Attributing liability to avatars poses significant challenges due to their potential anonymity and AI-driven autonomy.[19] Avatars may act independently of their users, especially in cases involving machine learning (ML) or artificial intelligence (AI), complicating accountability.[20] For instance, an AI-controlled avatar committing harassment raises questions about whether liability lies with the user, the platform, or the AI developer.[21] Anonymity further hinders identification, as users can create multiple avatars or use pseudonymous identities, undermining traditional investigative methods.[22]

4. Case Studies of Metaverse Offences:

4.1 Virtual Sexual Assault

Virtual sexual assault, or "meta-rape," involves non-consensual interactions between avatars that mimic sexual violence, often amplified by haptic technologies.[23] A notable case is Nina Patel's 2021 experience in Meta's Horizon Worlds, where her avatar was verbally and sexually assaulted, causing psychological distress akin to real-world assault.[24] Similarly, the 2024 UK case of a minor's avatar being gang-raped highlighted the emotional impact of such offences, yet legal recourse was limited due to the inapplicability of physical assault laws.[25] These incidents underscore the need for laws recognizing virtual acts as extensions of real-world harm.

4.2 Financial Crimes and Fraud

The metaverse's integration with cryptocurrencies and NFTs has facilitated financial crimes, including scams and money laundering.[26] For example, fraudulent NFT transactions have led to significant economic losses, with victims often unable to seek redress due to decentralized platforms and lack of regulation.[27] The anonymity of blockchain transactions further complicates tracing perpetrators, necessitating robust anti-money laundering (AML) frameworks tailored to virtual assets.[28]

4.3 Identity Theft and Data Breaches

The metaverse collects extensive personal data, such as biometric information and behavioral patterns, increasing the risk of identity theft.[29] Incidents of avatar hijacking and unauthorized data sharing have been reported, with platforms like Roblox facing lawsuits for harassment and data breaches.[30] The EU's General Data Protection Regulation (GDPR) may apply, but its provisions require clarification to address metaverse-specific data processing.[31]

5. Current Legal Frameworks and Their Limitations:

5.1 National Laws: UK, EU, and Beyond

In the UK, 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 struggles with virtual contexts.[32] The proposed Online Safety Bill (2021) aims to regulate harmful content but lacks specificity for metaverse interactions.[33] In the EU, the Draft AI Regulation addresses high-risk AI systems but does not cover avatar-based offences comprehensively.[34] South Korea's Act on Special Cases Concerning the Punishment of Sexual Violence Crimes is similarly limited to physical contexts, leaving virtual offences unaddressed.[35] India's Information Technology Act 2000 applies to online content but fails to account for the immersive nature of metaverse crimes.[36]

5.2 International Legal Instruments

The Budapest Convention on Cybercrime (2001) provides a framework for cyber-enabled offences but does not explicitly address metaverse-specific issues like avatar liability or virtual harm.[37] INTERPOL's 2024 guidelines categorize metacrime but lack enforceable mechanisms.[38] Proposals for a Metaverse Grand Charter of Laws suggest a cross-border e-jurisdiction, but implementation remains challenging due to differing national priorities.[39]

6. Towards a Comprehensive Legal Framework:

6.1 Adapting Existing Laws

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.[40] Similarly, data protection laws like GDPR could be revised to address metaverse-specific data, such as biometric and behavioral information.[41]

6.2 International Cooperation and E-Jurisdiction

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.[42] Blockchain-based identity verification could enhance traceability while respecting privacy, supported by international treaties modeled on the Budapest Convention.[43]

6.3 Industry Self-Regulation and Technological Solutions

Industry self-regulation, such as Meta's "personal boundary" feature, can mitigate harms but is insufficient without binding standards.[44] Technological solutions, like AI-driven content moderation and forensic tools for evidence collection, could enhance policing capabilities.[45] Platforms should also implement mandatory avatar registration to reduce anonymity and ensure accountability.[46]

7. Conclusion:

The metaverse represents a transformative digital frontier, but its potential is marred by the rise of metacrime, which exploits the legal vacuum in virtual spaces. Jurisdictional ambiguities, the absence of corporeal elements, and avatar anonymity challenge traditional criminal law, leaving victims of virtual offences without adequate recourse. By adapting national laws, fostering international cooperation, and leveraging industry self-regulation, policymakers can bridge the gap between virtual crime and real punishment. Recognizing avatars as extensions of legal personality and developing metaverse-specific regulations are critical steps toward ensuring a safe and equitable digital ecosystem. As the metaverse evolves, so must the law, lest it become a sanctuary for impunity.

References

[1] Neal Stephenson, *Snow Crash* (Penguin, 1992).

[2] GD Ritterbusch and MR Teichmann, 'Defining the Metaverse: A Systematic Literature Review' (2023) 11 IEEE Access 12368.

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

[4] 'Virtual Gang Rape Reported in the Metaverse' The Hindu (4 January 2024) <www.thehindu.com>.

[5] Ritterbusch and Teichmann (n 2).

[6] Ibid.

[7] 'Crime and Punishment in the Metaverse: A Primer' (ORF, 2 January 2024) <www.orfonline.org>.

[8] INTERPOL, 'Metaverse Crime Classification' (2024) <www.interpol.int>.

[9] 'From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse' (2025) Oxford Journal of Legal Studies.

[10] Centre for Countering Digital Hate, 'Metaverse Report' (2022) <counterhate.com/metaverse>.

[11] INTERPOL (n 8).

[12] 'Challenges in the Metaverse Jurisdiction and International Treaty Law' (2023) IRPJ 1.

[13] Ibid.

[14] 'Metaverse Policing: A Systematic Literature Review' (2023) ScienceDirect.

[15] Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185.

[16] Sexual Offences Act 2003, s 3 (UK).

[17] 'Policing the Metaverse: The Reality of Virtual Sexual Offences' (Kingsley Napley, 31 January 2024) <www.kingsleynapley.co.uk>.

[18] The Hindu (n 4).

[19] 'Crime and Punishment in the Metaverse' (n 7).

[20] Ibid.

[21] 'Identity, Crimes, and Law Enforcement in the Metaverse' (2025) Humanities and Social Sciences Communications.

[22] 'Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality' (2024) Asian Journal of Criminology.

[23] Oxford Journal of Legal Studies (n 9).

[24] 'The Metaverse: Virtual Offences, Real World Penalties?' (Kingsley Napley, 9 June 2022) <www.kingsleynapley.co.uk>.

[25] The Hindu (n 4).

[26] 'Metaverse Crimes in Virtual (Un)reality: Fraud and Sexual Offences under English Law' (2023) ScienceDirect.

[27] Ibid.

[28] 'Challenges in the Metaverse Jurisdiction' (n 12).

[29] 'Redefining Boundaries in the Metaverse' (2024) MDPI.

[30] Kingsley Napley (n 24).

[31] General Data Protection Regulation (EU) 2016/679.

[32] Protection from Harassment Act 1997, s 2 (UK).

[33] 'Challenges in the Metaverse Jurisdiction' (n 12).

[34] EU Draft AI Regulation (2021).

[35] 'Redefining Boundaries in the Metaverse' (n 29).

[36] Information Technology Act 2000 (India).

[37] Budapest Convention (n 15).

[38] INTERPOL (n 8).

[39] 'Metaverse: Model Criminal Code' (2023) ResearchGate.

[40] Oxford Journal of Legal Studies (n 9).

[41] GDPR (n 31).

[42] Swedish Criminal Code, Chapter 6, s 7.

[43] 'Metaverse: Model Criminal Code' (n 39).

[44] Kingsley Napley (n 24).

[45] 'Metaverse Policing' (n 14).

[46] 'Crime and Punishment in the Metaverse' (n 7).