INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER CRIMES IN METAVERSE: EMERGING LEGAL CHALLENGES IN A VIRTUAL WORLD

AUTHORED BY - NILA SUNIL LAL

Abstract

The emergence of the Metaverse—a shared, immersive digital ecosystem powered by virtual reality (VR), blockchain, and artificial intelligence (AI)—has redefined the way people interact, socialize, work, and transact online. While this new frontier promises innovation and connection, it also gives rise to complex challenges, particularly in the realm of cyber crime. This paper seeks to explore the evolving nature of cyber crimes within the Metaverse, an ecosystem where avatars serve as identities and virtual assets hold real-world value.

The study begins by examining the rise in cyber activities within virtual platforms such as Decentraland, Meta Horizon Worlds, and Roblox, which have become fertile grounds for digital interactions and unfortunately, criminal exploitation. It then delves into how traditional cyber crimes—such as identity theft, phishing, harassment, and financial fraud—are adapting to this immersive environment, taking on new forms like avatar impersonation, NFT scams, and cyber sexual assault in VR spaces. The paper also categorizes emerging types of Metaverse-specific crimes, including unauthorized access to digital assets, voice cloning for manipulation, and privacy invasions via biometric tracking.

In doing so, the research humanizes the impact of these crimes on individuals, many of whom face emotional distress, social embarrassment, or financial loss despite the perceived "virtual" nature of the space. Furthermore, the paper evaluates the gaps in current cyber laws and digital governance, questioning whether traditional legal frameworks can truly protect users in such decentralized, fast-evolving environments. Through this exploration, the paper calls for a more nuanced, globally cooperative legal approach to safeguarding human rights and user autonomy in the Metaverse.

KEYWORDS; Metaverse, Cyber Crime, Virtual Reality Law, Digital Identity Theft, Online Safety

ISSN: 2582-6433

Introduction

Metaverses are engaging three-dimensional virtual environments where individuals interact as avatars, both with one another and with software agents, mimicking the real world while transcending its physical constraints (Davis et al., 2009). The term 'metaverse' was first introduced in Neal Stephenson's 1992 science fiction novel, Snow Crash, where it described an expansive virtual realm that exists alongside the physical world (Stephenson, 2003). The idea of the Metaverse pertains to a collective, enduring virtual world where individuals can engage with one another similarly to how they do in the physical world (Guan et al., 2022). The Metaverse is frequently characterized as an advanced development of the Internet. Unlike websites and applications that mainly depend on 2D interfaces, the metaverse is transitioning into engaging 3D environments. Users have the ability to interact in real-time, explore diverse worlds, purchase digital items, and even live a virtual existence represented by avatars. The Metaverse integrates a range of technologies including virtual reality (VR), augmented reality (AR), blockchain, artificial intelligence, and social media.

The word indicates using of VR and AR technology to interact rather than using mobile, laptops and desktops (Sparkes, 2021). The beginning can be traced back to times when the World wide web was created by Tim Berners to connect the internet by a web browser which further expanded to the activities such as sending mails and then it even went further for the creating of different social media platforms, the concept of metaverse is that the people can not only just view but for an immersive experience (Berners- lee et al., 1992). Metaverse will be for work, education, health, conferences, or even just hanging out (Nover, 2021).

Augmented Reality (AR) is a technology that enhances the real-world environment around us by overlaying computer-generated content onto it (Hantono et al., 2018), for professional applications across various fields, including healthcare, manufacturing, education, and retail (Antonioli et al., 2014). Organizations are increasingly utilizing AR to enhance employee safety through virtual training simulations and by visualizing the functionality of equipment prior to its production. Conversely, Virtual Reality (VR) represents a cutting-edge technological advancement that has transformed our experiences and interactions within digital environments (Velev & Zlateva, 2017). Virtual Reality (VR) immerses users in an entirely new digital realm, offering an interactive experience via headsets or glasses. Augmented Reality (AR) enhances the real-world environment by superimposing digital objects onto it, enriching it with additional information or improving its functionality. Augmented Reality (AR) and

ISSN: 2582-6433

Virtual Reality (VR) technologies can be utilized to develop virtual environments and simulations, enabling students to investigate and engage with real-world settings without having to exit the classroom (Young et al., 2020).

Virtual spaces

As the idea of the Metaverse evolves from mere fiction to practical digital realms, numerous prominent platforms have surfaced as key virtual spaces for social engagement, economic transactions, and immersive experiences.

i) Meta Horizons Worlds

Horizon is a virtual reality-based online video game and game creation platform, exclusively available on Meta VR headsets. Created and released by Meta Platforms, this game enables players to engage with one another across different worlds, where they can take part in events, games, and social interactions. The Meta Privacy Policy regulates privacy within Meta's Horizon Worlds, where user-generated content, messages, interactions, purchases, and additional data are collected for purposes such as personalization, enhancement, safety, and research. This includes data pertaining to Meta Horizon Profiles (such as profile name, image, interactions), physical attributes and movements (like headset position, audio data), device details, Meta VR Product activities (including purchases, events attended), content generation, fitness data, gameplay metrics, environmental information, camera and audio details, voice interactions, and data from third parties (Meta, n.d.). legal concern is virtual sexual harassment cases, and such cases have already been reported.

ii) Decentraland

Decentraland is an exquisite virtual reality platform, elegantly built on the Ethereum blockchain, enabling users to craft, immerse themselves in, and profit from their unique virtual reality content and applications. This sophisticated platform features its own cryptocurrency, MANA, serving as the principal currency for the acquisition and sale of virtual assets, as well as for engaging in the vibrant economy of the platform. Within Decentraland, users have the opportunity to design and possess their own virtual parcels of land, referred to as LAND, which are represented as non-fungible tokens (NFTs) on the Ethereum blockchain. In the realm of AI integration, the Decentraland Decentralized Autonomous Organization (DAO) has graciously sanctioned a grant proposal aimed at financing the creation of DCL Builder AI, an innovative AI tool

ISSN: 2582-6433

designed to generate scenes and various assets using natural language prompts (Whelan, 2023). The legal concerns include NFT scams, property fraud and lack of regulatory framework.

iii) Sandbox

The Sandbox is a virtual 3D world where users can create experiences. The platform is blockchain-based and emphasizes monetization of the user's creations and an in-world economy. In-game currency may be exchanged for fiat currency (Madrid et al.,). There are no other connections to the tangible world. Engaging in live interaction is feasible solely with a restricted number of users present on the same parcel of land simultaneously. The legal concerns are money laundering and lack of accountability.

iv) Fortnite

Fortnite made its debut in the market in July 2017 as a collaborative survival shooter, crafted by the esteemed Epic Games. Fortnite can be enjoyed across a multitude of platforms, such as PC, PlayStation, and mobile devices. Epic Games, the creator of Unreal Engine, provides a game engine that is widely utilized by numerous game developers. This promotes seamless interoperability. The legal issue includes IP issues, virtual content regulation.

The rise of cyber activities in metaverse

The inaugural generation of the World Wide Web, known as Web 1.0, was distinguished by its open protocols, open-source codes, and communal forums (Drake, 2022). The advent of Web 2.0 in the early 2000s introduced content-centric websites alongside the burgeoning mobile internet. Nevertheless, platforms such as Facebook, Google, and Twitter, dominated by major corporations, established a virtual monopoly within this domain. The forthcoming Web 3.0 aspires to create decentralised workspaces and promises fully immersive experiences through the Metaverse. (Drake, 2022).

The Metaverse represents an evolved iteration of the Cyber-Physical Social System, wherein physical systems, human society, and cyber systems are intricately linked through complex interactions (Zhou et al.,). It is projected that the Metaverse will undergo a complete evolution through four expansive stages (Centieiro, 2022).

ISSN: 2582-6433

Stage 1: Virtual reality (VR) technology will enable users to engage with visuals and sounds within the Metaverse. This initial stage is predominantly led by gaming enterprises. The emergence of blockchain, cryptocurrencies, and non-fungible tokens (NFTs) has also propelled the Metaverse's progress, fostering a heightened interest in possessing unique digital assets anchored in blockchain, such as 'skins' for avatars in gaming realms.

Stage 2: The second stage aims to enhance sensory immersion through a blend of movement and touch-enhancing apparatus, such as haptic suits, (Haptic, 2022) allowing the wearer to simulate motion.

Stage 3: The third stage endeavours to employ what is sometimes referred to as advanced VR to replicate real-world experiences by transmitting information directly to the brain via neural signals. An illustrative case would be the application of virtual environments and reality for pain management in clinical patients (Shahrbanian et al.,) Gathering neural data in response to stimuli presented in VR, although not yet standard practice, is another emerging field (currently under exploration by companies like Neuralink. The ultimate ambition is to "transport consciousness" without the need to move the body.

i) Workplace

Employees connect with their colleagues via virtual video meetings. Yet, the persistent reliance on these interactions can become tiresome over time. The Metaverse offers a solution, enabling employees to engage in more genuine interactions that alleviate this fatigue. Owing to its immersive and captivating experience, the Metaverse has the potential to mitigate several of these issues, such as reducing reliance on personal camera feeds and alleviating limitations imposed by physical mobility. Furthermore, with the advent of realistic interactions that are less taxing and more genuine, incorporating the Metaverse into the daily work routine will become increasingly effortless.

ii) Education

As a captivating virtual realm, the concept of the Metaverse has the potential to transform campus activities and class lectures through 3D simulations, facilitating a more authentic classroom learning experience where all participants engage in an immersive manner (Iqbal et al., 2023). The system is designed to offer an immersive

ISSN: 2582-6433

on-campus Metaverse experience for students, blending a mixed environment where their real-world actions resonate within the virtual realm (Duan et al., 2021)

iii) Gaming Industry

In a groundbreaking shift, the gaming sector is embracing decentralization. Play-to-earn games can provide players with digital identity, assets, and ownership within the virtual realm (Brambilla, 2021).

iv) Entertainment

Metaverses will empower experience-driven entertainment brands to explore virtual venues that go beyond the constraints of physical locations, unveiling new forms of experiences (Pietroszek et al., 2021). In the year 2021, the renowned US reality television personality Paris Hilton unveiled her Metaverse venture on Roblox. Her digital realm, known as Paris World, invites guests to navigate through virtual replicas of her opulent Beverly Hills estate, whether in a luxurious sports car or aboard a Sunray yacht (Dawn, n.d.).

v) Healthcare

In the realms of healthcare and medicine, immersive technologies have demonstrated their efficacy in providing realistic and interactive simulations (Coyne et al., 2021). A Metaverse dedicated to the Burn Hospital has been created on the Gather Town platform to facilitate a range of lectures and workshops (Hwang, 2023).

The aim of this paper is to meticulously scrutinize the burgeoning issue of cybercrimes within the Metaverse—a swiftly evolving virtual realm that intertwines social, economic, and technological interactions within immersive 3D settings. As individuals participate through avatars and engage in transactions utilizing virtual currencies and assets, the distinctions between the digital and physical realms increasingly dissolve, leading to the emergence of unprecedented cyber threats. This paper endeavours to investigate the characteristics and extent of such crimes, evaluate the sufficiency of current legal frameworks in tackling these challenges, and underscore the pressing necessity for policy reform. By delving into key platforms, pinpointing prevalent patterns of misconduct, and assessing both national and international legal responses, the paper aspires to enrich the ongoing dialogue surrounding digital safety, privacy, and accountability in virtual environments. Ultimately, this study aims

ISSN: 2582-6433

to cultivate heightened awareness and promote the development of informed, forward-thinking legal solutions to safeguard users within the expanding Metaverse landscape.

Understanding Cyber Crimes in the Metaverse

Cybercrime' encompasses actions carried out in the digital realm. In essence, it pertains to any endeavour where electronic communication devices (ECDs) or networks serve as instruments, targets, or venues for illicit activities. The definition of cybercrime includes offenses against the confidentiality, integrity, and availability of data and computer systems, traditional crimes associated with computers, content-related violations, and offenses concerning copyright and privacy infringement. With the swift advancement of information and communication technologies (ICTs) across nearly all aspects of human endeavour, coupled with the continually rising number of IT users, the likelihood of cyber assaults on information systems (targets) is escalating, leading to significant damage and substantial revenue losses. The individuals engaged in cybercrime often partake in these activities driven by a sense of curiosity and amusement, or at times, purely for the purpose of financial gain. Cyberattacks are carried out swiftly and possess the capability to impact countless devices globally within a brief period. Furthermore, any system may be susceptible to threats posed by employees within the organization itself. It is a well-acknowledged fact that the only truly secure computer is one that is entirely isolated from any network and is not accessed by others. It is imperative that all personnel in the IT department, along with those in any organization possessing IT infrastructure, are aware of the potential dangers and ensure that comprehensive security policies are put in place. However, the complex nature of technology and the vastness of cyberspace make the identification of cybercrime a challenging endeavour. Tackling cybercrime requires specialized expertise and training to gather evidence, follow appropriate protocols for the analysis and validation of the offense, and ultimately present it in a court of law to ensure that cybercriminals are held accountable (Dejey & Murugan, 2018).

Cyber crimes related to virtual sexual harassment /avatar molestation

The concept of 'virtual rape' first surfaced in 1993 within the digital realm of LambdaMoo, where an individual employed a text-driven application to manipulate other avatars into articulating graphic sexual actions and participating in sexual conduct (Strikwerda,2015). In the year 2007, the Belgian Federal Police embarked on a criminal inquiry regarding a ‘virtual rape’ occurrence within the realms of Second Life, a virtual reality platform, where one avatar enacted non-consensual sexual acts by seizing control of another avatar. While no formal

ISSN: 2582-6433

charges were filed, this case illuminated the frequency of such incidents, marking an early glimpse into the complexities of the metaverse (Danaher, 2018). As technology advanced and gained widespread acceptance, reports began to attract significant media attention. In 2016, Jordan Belamire recounted her experience of being groped in QuiVr, a virtual reality game. Although she was only identifiable as a woman through her voice, another player approached her avatar, started to caress her chest, pursued her, and attempted to reach towards her avatar's crotch. Belamire stated that she instructed the offender to cease his actions, and she perceived the abuse as 'real', 'frightening', and 'violating' (Belamire, 2024).

When examining personal accounts of sexual violence and harassment within the metaverse, the stories frequently reflect well-known themes, mirroring accounts of events that transpire in the physical realm. Typically, the female-presenting avatar, acting as the victim, endures non-consensual touching, groping, exposure to ejaculatory acts, or penetration inflicted by one or more male avatars. These actions may entail varying levels of force and coercion, occur in the presence of onlookers, and are sometimes recorded through filming or photography (Donegan, 2023). It is important to note that the victim's reactions to sexual violence and harassment within the metaverse closely reflect offline responses, frequently encompassing moments of freezing and fleeing (Yoon, 2022). The reasons appear to be threefold. Firstly, the customization of avatar bodies can foster profound psychological connections, resulting in the effects of abuse lingering beyond the virtual realm, manifesting in tangible physical reactions such as anxiety, panic attacks, and possible depression similar to that experienced by real-life victims (Ramirez et al., 2023).

Identity theft and impersonation of avatars

Identity Theft denotes the unauthorized use of someone else's personal identity details, including their name, number, credit or debit card information, and more, with the intent to perpetrate fraud. This nefarious act is frequently executed through methods such as phishing, skimming, data breaches, and phone scams, utilizing channels like emails, social media, point-of-sale devices, mobile phones, and similar platforms. The offense of identity theft is addressed under Section 66C of the Information Technology Act, defined as the fraudulent or dishonest utilization of another individual's electronic signature, password, or any other distinctive identification characteristic. Safeguarding against identity theft necessitates the confirmation that purchasers are indeed who they assert to be. Vendors and lenders utilize an array of methods to accomplish this objective. Authentication methods can be categorized into three

ISSN: 2582-6433

distinct types: "token-based" authentication, which relies on a tangible item held by the user; "knowledge-based" authentication, which depends on information that only the individual is presumed to possess; and biometrics, which is founded on a unique physical trait of the individual, such as their signature style (Clarke, 1994). Identity theft has emerged as a favoured crime among wrongdoers, as it offers perpetrators the opportunity for an exceptionally high reward while simultaneously presenting a remarkably low risk of being caught.

A significant factor contributing to the increase of this crime is the effortless accessibility to individuals' personal information from myriad sources. These include government entities, healthcare facilities, payment card companies, mobile service providers, and various commercial organizations that routinely gather and retain data, often lacking adequate safeguards.

The digital landscape has transformed the way we present ourselves in the online realm. Avatars have become essential to our virtual identities. As we increasingly immerse ourselves in the digital world, the risk of avatar identity theft escalates (Guildhawk, 2024). Overseeing digital identities is becoming increasingly challenging. Research indicates that 40% of organizations encounter identity-related problems due to digital avatars. The market for digital identities is projected to expand by 20% annually. This underscores the critical importance of robust security measures. Cyber identity theft can be elegantly defined as the illicit and unauthorized exploitation of an individual's personal information or digital person (Chawki et al., 2024). Within the realm of the metaverse, the concept transcends mere identity theft as it is commonly understood. Users engage with one another across unique platforms, extending beyond basic personal information like names and addresses. Virtual assets can encompass avatars, individual preferences and aversions, purchasing histories, or even biometric characteristics such as facial recognition and the tracking of a person's movements within the metaverse (Shahriar, 2024). The existence of various diversified avatars within the metaverse environment elevates the potential for theft risk. The initial concern is Virtual Avatars Security Issues. The research revealed that these avatars are employed by cybercriminals for impersonation, financial fraud, or social engineering attacks (Rashid and Khan, 2024). Another notable reason highlighted by the authors for digital identity theft in virtual realms is the inadequate authentication processes. Studies indicate that a majority of current metaverse applications continue to rely on conventional security measures such as Single Factor Authentication (SFA) or merely simplistic security frameworks ((Awadallah et al., 2023). The

ISSN: 2582-6433

dependence on easily circumvented security protocols, such as usernames and passwords, exposes users to significant risks of exploitation. Furthermore, the decentralized nature of numerous pliable metaverse platforms means that no singular authority is responsible for safeguarding user data, thereby increasing the likelihood of malicious actors taking advantage of existing vulnerabilities ((Pooyandeh et al,2022).

Phishing and Malware Inside Games and VR events

In recent years, the emergence of online gaming and virtual reality (VR) environments has unveiled a plethora of new cybersecurity threats. As these platforms gain popularity and become more immersive, they simultaneously transform into enticing targets for cybercriminals. Among the most alarming threats are phishing schemes and the proliferation of malware within games and VR events. These attacks not only jeopardize user data and privacy but can also result in extensive network vulnerabilities and significant financial losses. Phishing is a type of cyberattack where individuals are tricked into giving up personal details like login information, credit card numbers, or other sensitive data. In gaming and virtual reality (VR) environments, phishing typically shows up as fake messages, suspicious links, or users pretending to be someone they're not. For instance, a player might get a message that looks like it's from a game moderator or another player, asking them to click a link to claim a free item or verify their account. These links often lead to fake websites designed to steal their login credentials (Srinivasan, 2021).

What makes phishing even more dangerous in VR is how immersive the experience is. In virtual spaces, avatars can be made to look and sound very real, making it much harder to tell who's legitimate and who isn't. Some attackers even use voice-changing technology or ultra-realistic avatars to trick users. According to the Cybersecurity and Infrastructure Security Agency (CISA), VR platforms are especially vulnerable because they often lack strong tools for verifying users' identities (CISA, 2023).

Adding to the problem, many online games and VR platforms involve financial transactions, like buying digital items or premium content. Since users often save their payment information within these platforms, a successful phishing attack can have serious financial consequences.

ISSN: 2582-6433

How the Industry Is Responding

To tackle these threats, developers of games and VR platforms are being pushed to step up their security measures. This includes using multi-factor authentication, monitoring network activity in real time, and being more selective about the third-party content allowed on their platforms. But tech fixes alone aren't enough—users also need to be aware of the risks. It's important for players to be cautious about unexpected messages, avoid clicking on links from unfamiliar sources, and only install software from official or well-known providers.

Government agencies and cybersecurity organizations are starting to take more action too. The European Union Agency for Cybersecurity (ENISA), for example, has begun drafting security guidelines for VR and gaming platforms. These recommendations emphasize the use of encryption, strong identity verification, and isolating risky or unknown code to reduce the chance of attacks (ENISA, 2023).

As gaming and VR technologies continue to blend into everyday life, whether for entertainment, education, or business, securing these platforms is more important than ever. If companies and users don't take steps to address these evolving threats, it could weaken public trust and slow down the growth of what are otherwise very promising technologies.

Digital Asset Theft

According to the U.S. Securities and Exchange Commission (SEC), a digital asset is defined as: An asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "Virtual currencies," "coins," and "tokens. One of the most intricate challenges faced both worldwide and within India is the legal categorization of digital resources. The absence of a universally recognized classification results in varied legal interpretations. While India does not possess a specific law that delineates digital assets, the Income Tax Act, following the amendments in 2022, refers to them as "Virtual Digital Assets (VDAs)".

Virtual assets embody ownership or value encapsulated in a digital format. These encompass: Cryptocurrencies: Bitcoin, Ethereum, and a myriad of altcoins traded on a global scale. Non-Fungible Tokens (NFTs): Distinctive digital collectibles, art pieces, music, and even virtual fashion items. Virtual Real Estate: Digital parcels and properties situated within metaverse platforms such as Decentraland or The Sandbox. Gaming Assets: In-game currencies, rare

ISSN: 2582-6433

items, and avatars that possess significant monetary value. The worldwide market capitalization of these assets has now soared into the trillions of dollars, drawing investors from diverse backgrounds. Nevertheless, this remarkable growth also entices cybercriminals driven by the lucrative prospects of successful heists. A multitude of elements contribute to the surge in virtual asset theft: Decentralization and Irreversibility, the decentralized essence of blockchain technology eliminates centralized intermediaries and the possibility of reversing transactions. Once a transfer occurs, it is irrevocable, rendering theft permanent and making recovery a formidable challenge. Lack of Regulation and Oversight, Numerous jurisdictions are devoid of explicit laws that govern digital assets, which restricts legal recourse for victims and fosters an environment conducive to criminal activity. Increasing Sophistication of Cybercriminals, Cybercriminals are perpetually enhancing their tactics, employing sophisticated phishing schemes, malware, social engineering, and exploit techniques.

Growth of DeFi and Metaverse Platforms, the swift expansion of decentralized finance (DeFi) and metaverse platforms introduces a plethora of new attack vectors, including vulnerabilities in smart contracts and deceptive virtual asset sales.

In the case of a 41-year-old Chinese man, Qui Chengwei, who was an active participant in the virtual realm of Legend of Mir II, he had acquired a notably rare weapon, the Dragon Sabre, during an online quest. Subsequently, he lent this weapon to another individual, Zhu Caoyuan, who, without authorization, sold it for roughly $1000 (NZ). Had the Dragon Sabre been a tangible item, Caoyuan would have been guilty of theft by conversion. However, when the aggrieved party initially approached the police for assistance, he was informed that the theft did not constitute a crime, as virtual property was not recognized as a protectable asset under the prevailing laws at that time (Lee, 2002). Following this, Chengwei confronted the alleged thief at his home, stabbing the 26-year-old Caoyuan multiple times, resulting in his death. Despite Chengwei receiving a death sentence for this very real act of murder, the case holds significant relevance in the realm of virtual theft for two primary reasons. Firstly, it exemplifies one of the methods through which theft can transpire within a virtual environment. A user (or their avatar) may acquire another user's virtual possessions, either with limited permission or through deceit. While such possession may not inherently qualify as theft, if the items are utilized or handled in a manner that infringes upon the owner's rights, the offense of theft could, in theory, be applicable. Secondly, this high-profile case drew both political and public scrutiny towards the issue of legal safeguards for virtual property. Digital currency, particularly

ISSN: 2582-6433

decentralized cryptocurrencies such as Bitcoin, introduces unparalleled challenges for regulation owing to its inherent anonymity and the nature of cross-border transactions. Given that digital currency transactions can circumvent conventional financial institutions and that transaction records are preserved on distributed ledgers, monitoring the movement of funds becomes progressively more complex (Lifang, 2024).

Common Techniques for Virtual Asset Theft: Phishing Attacks, Cybercriminals masquerade as legitimate organizations to deceive victims into disclosing private keys, seed phrases, or login credentials via counterfeit websites, emails, or messages. Malware and Keyloggers, Harmful software installed on devices can capture keystrokes or access wallet files, surreptitiously stealing sensitive information. Social Engineering, Criminals exploit psychological manipulation to persuade victims into willingly granting access, often by impersonating support personnel or trusted figures within communities. Exploiting Smart Contract Vulnerabilities, Deficiencies in smart contracts—self-executing blockchain protocols—can be manipulated to siphon off funds or alter transactions. Fake ICOs and Investment Scams, Deceptive initial coin offerings or fraudulent investment schemes promise substantial returns but ultimately misappropriate funds from investors. SIM Swapping, Cybercriminals seize control of a victim's mobile phone number to circumvent two-factor authentication (2FA) and gain entry to accounts.

Legal Challenges of Cybercrimes in the Metaverse

The metaverse, a virtual space where people interact through avatars in real time, is rapidly transforming how we socialize, work, and do business. But as exciting as this digital frontier is, it comes with serious legal complications—especially when it comes to handling cybercrimes. The nature of the metaverse raises questions about jurisdiction, user identity, regulation, and the legal status of digital assets, all of which make enforcing laws incredibly difficult.

One of the most pressing issues is jurisdiction. In the physical world, laws are enforced within national borders. But in the metaverse, a crime could involve a user in India interacting with a server based in the U.S., all hosted by a company registered in Ireland. This makes it unclear which country has the authority to investigate and prosecute the offense. Cross-border cybercrime isn't new, but the metaverse amplifies the problem because of its complex, decentralized structure (Kshetri, 2022).

ISSN: 2582-6433

Another major challenge is identifying the real individuals behind avatars. In many virtual platforms, users can create and operate avatars without revealing their real names or locations. If someone commits harassment, fraud, or even virtual assault, tracking them down becomes incredibly difficult. Unlike traditional social media, where accounts often tie to phone numbers or emails, the metaverse can operate with even less traceable identity verification (Terry, 2023). This anonymity not only shields bad actors but also complicates the process of collecting digital evidence that would hold up in court.

A core legal gap is that no country currently has a comprehensive law that specifically addresses crimes in the metaverse. Existing cyber laws were created long before immersive virtual worlds became common. For example, many legal systems don't define what constitutes property damage or personal harm in a virtual environment. If a person's digital assets are stolen, or if their avatar is targeted in a harmful way, it's unclear how—or even if—those actions are legally punishable under current laws (Hughes, 2023).

Moreover, the regulation of virtual currencies and assets is still developing. Many metaverse platforms use digital currencies to buy, sell, and trade goods. But because these currencies are often unregulated, they're vulnerable to scams, theft, and money laundering. Without oversight from financial authorities, it's hard to trace illegal transactions or recover stolen digital funds (Chohan, 2021).

Finally, the lack of surveillance and enforcement tools within VR platforms makes it even harder to monitor criminal behaviour. Unlike traditional websites, VR spaces often don't record interactions or store logs that can be reviewed later. This limits law enforcement's ability to investigate reported incidents and hold offenders accountable.

In short, while the metaverse opens up new possibilities, it also exposes deep flaws in current legal systems. Until governments create laws specifically designed for virtual environments and improve international cooperation, cybercrimes in the metaverse will remain difficult to detect, prove, and prosecute.

Existing Legal Frameworks: India and Global

As the digital world rapidly expands into immersive environments like the metaverse, questions around legal protections and enforcement are growing louder. While some legal structures do

ISSN: 2582-6433

exist—both in India and globally—they were not designed with the metaverse in mind. This creates significant gaps in regulation, especially when it comes to protecting users from cybercrime in virtual spaces.

In India, the Information Technology Act, 2000 is the primary law governing cyber activities. Several sections of the Act are relevant to virtual environments. For example, Section 66E deals with privacy violations, including the capturing or publishing of private images without consent. Section 67A criminalizes the publication of sexually explicit content in electronic form, which could apply to VR interactions that cross legal or moral boundaries. The Indian Penal Code (IPC) is also applicable in some digital contexts, especially where offenses like criminal intimidation or fraud are involved (Ministry of Electronics and Information Technology [MeitY], 2023). However, these laws were not written with the immersive and anonymous nature of the metaverse in mind.

India's new Bharatiya Nagarik Suraksha Sanhita (BNSS), aimed at modernizing the criminal justice system, still lacks clear guidelines for addressing crimes that happen entirely in virtual spaces. For instance, what happens if someone is harassed in the metaverse using avatars or if virtual property is stolen? Current legal texts offer no clarity on how to prosecute such offenses, especially when physical harm isn't involved.

Globally, the picture isn’t much clearer. In the European Union, the General Data Protection Regulation (GDPR) remains one of the most robust frameworks for data protection. It provides users with rights over their personal data and places obligations on companies to handle that data responsibly. While this could technically apply to metaverse platforms operating in the EU, the regulation doesn’t specifically address virtual reality environments (European Commission, 2018).

In the United States, various cybersecurity laws exist, such as the Computer Fraud and Abuse Act (CFAA), but enforcement varies widely by state. U.S. law tends to be reactive rather than proactive in the face of emerging technology. Interpol, meanwhile, has launched global cybercrime initiatives to improve international collaboration, but again, no global body has produced a specific framework for crimes occurring in the metaverse (Interpol, 2023).

The biggest issue globally is that there’s currently no unified legal framework for the

ISSN: 2582-6433

metaverse. Each country has its own rules for data protection, criminal activity, and digital identity—but when crimes happen across borders in decentralized platforms, enforcement becomes nearly impossible. Virtual spaces like the metaverse require new thinking around legal identity, digital ownership, and jurisdiction.

Until international laws catch up, the responsibility largely falls on individual platforms to create and enforce community guidelines. However, these rules don't carry the weight of law and can't substitute for legal accountability. Clearly, both national governments and global organizations need to step up and create laws that recognize the unique challenges of virtual spaces.

Way Forward

As the metaverse continues to evolve into a major part of our digital lives, it's clear that legal systems around the world must adapt quickly. The immersive, borderless nature of virtual environments makes them particularly vulnerable to exploitation. To create a safer and more accountable metaverse, several steps must be taken on both national and international levels.

First and foremost, there is a pressing need for new laws—or at the very least, amendments to existing ones—that specifically address virtual crimes. Most legal frameworks today are built around the assumption that crimes happen in the physical world. But what happens when harassment, theft, or fraud takes place entirely in a digital environment? Legislators need to recognize that harm can be real, even if it happens through avatars or virtual objects. Legal definitions should expand to include psychological harm, digital property rights, and online consent in immersive spaces (Kshetri, 2022).

Another critical area is the regulation of digital identity. In the metaverse, users can easily hide behind anonymous or fabricated identities, making it hard to track down offenders. While complete anonymity can protect privacy and freedom of expression, it also opens the door to abuse. A balanced approach is needed—one that protects user privacy while ensuring platforms have tools to verify identities when required by law enforcement. Governments might consider establishing secure, privacy-respecting digital ID systems that could be used across virtual platforms (Hughes, 2023).

Equally important is the development of clear content moderation policies for VR platforms.

ISSN: 2582-6433

Unlike traditional social media, VR environments involve real-time voice, gesture, and body language interactions, which are harder to moderate. Platforms need to invest in tools and teams that can monitor inappropriate or abusive behaviour without infringing on users' rights. Moderation in VR isn't just about blocking harmful content; it's also about ensuring respectful communication in a space that feels real to its users (Terry, 2023).

On a broader level, international cooperation will be key. Since most metaverse platforms operate across borders, no single country can regulate them effectively on its own. International bodies, such as the United Nations or Interpol, should take the lead in forming coalitions and treaties that define acceptable conduct, data sharing protocols, and cross-border enforcement strategies (Interpol, 2023).

Finally, the role of artificial intelligence (AI) in safeguarding virtual spaces cannot be overlooked. AI-powered systems can help detect abusive language, gestures, or behaviour patterns in real time. When combined with human moderators and proper user reporting tools, AI can be a powerful ally in preventing harm before it escalates.

Legal recognition of harm experienced in virtual spaces is long overdue. Whether it's emotional distress caused by online harassment or financial loss through digital fraud, the consequences for users are real. A forward-thinking legal framework should acknowledge this reality and offer meaningful paths to justice.

References

1. Guan, J.; Irizawa, J.; Morris, A. Extended Reality and Internet of Things for Hyper-Conne Proceedings of the 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts a New Zealand, 12-16 March 2022; pp. 163-168
2. Sparkes, M. What is a metaverse. New Sci. 2021, 251, 18. [CrossRef]
3. Stephenson, N. Snow Crash: A Novel; Spectra:Irvine, CA, USA, 2003.
4. Berners-Lee, T.; Cailliau, R.; Groff, J.F.; Pollermann, B. World-Wide Web: The information u [CrossRef
5. Nover, S. The Meaning of the 'Metaverse, and All the Terms You Need to Understand //qz.com/2089665/everything-you-need-to-know-to-understand-the-metaverse (accessed july 20)
6. meta onlinehttps://www.oculus.com/accesed on july 20

ISSN: 2582-6433

7. The Sandbox, Introducing The Sandbox Alpha: Step into the Metaverse! Your chance to join the launch of a new era of gameplay is fast approaching. (accessed: july 25 2025)
8. Josh Drake,"How We Can Finally Evolve from Web2 to Web3."
9. https://ieeexplore.ieee.org/document/8931796
10. Henrique Centieiro, "The Roles of VR, AR and MR on the Metaverse," Medium,july 15 2025
11. Haptic VR Suit and Glove with Force Feedback," Teslasuit, June 29, 2025, https://teslasuit.io/
12. shahnaz Shahrbanian et al., "Use of Virtual Reality (Immersive vs. Non Immersive) for Pain Management in Children and Adults: A Systematic Review of Evidence from andomized Controlled Trials," European Journal of Experimental Biology (2012), https://www.researchgate.net/profile/Shahnaz-Shahrbanian/publication/315740184_Use_of_virtual_reality_immersive_vs_non_immersive_for_pain_management_in_children_and_adults_A_systematic_review_of_evidence_from_randomized_controlled_trials/links/5a340974abfdcc769fd22817/Use-of-virtual-reality-immersive-vs-non-immersive-for-pain-management-in-children-and-adults-A-systematic-review-of-evidence-from-randomized-controlled-trials.pdf.
13. Iqbal, M.Z.; Campbell, A.G. AGILEST approach: Using machine learning agents to facilitate kinesthetic learning in STEM education through real-time touchless hand interaction. Telemat. Inform. Rep. 2023, 9, 100034. [CrossRef
14. Duan, H, Li, J.; Fan, S., Lin, Z., Wu, X.; Cai, W. Metaverse for social good: A university campus prototype. In Proceedings of the 29th ACM International Conference on Multimedia, Virtual Event, 20-24 October 2021; pp. 153-161.
15. Brambilla, S. What play-to-earn gaming can tell us about the future of the digital economy -And the metaverse. World Economic Forum, 20 july 2025.
16. Pietroszek, K.;Rebol, M., Lake, B. Dill Pickle: Interactive Theatre Play in Virtual Reality. In Proceedings of the 28th ACM Symposium on Virtual Reality Software and Technology, Sukuba, Japan, 27 july 2025 ;pp. 1-2.
17. Dawn C. U.S. Reality TV Star Paris Hilton Launches Metaverse Business on Roblox. Available online: https://www.reuters. com/business/media-telecom/us-reality-tv-star-paris-hilton-launches- metaverse-business-roblox-2025-7-20/ (accessed on 22 july 2025).

ISSN: 2582-6433

18. Coyne, E., Calleja, P., Forster, E.; Lin, F A review of virtual-simulation for assessing healthcare students' clinical competency. Nurse Educ. Today 2025,96, 104623.[CrossRef]
19. Litska Strikwerda, 'Present and Future Instances of Virtual Rape in Light of Three X Categories of Legal Philosophical Theories on Rape' (2015) 28 Philosophy & Technology 491,493; Richard MacKinnon, 'Virtual Rape' (2006) 2 Journal of Computer-Mediated Communication 0,3.
1. John Danaher, "The Law and Ethics of Virtual Sexual Assault' in Woodrow Barfield and Marc Blitz, Research Handbook on the Law of Virtual and Augmented Reality (Edward Elgar Publishing 2018) 363
20. Jordan Belamire, "My First Virtual Reality Groping' (Medium, 20 October 2016) <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee> accessed 24 July 2025
21. Guildhawk, Legal identity and Avatar representation: Safeguarding your digital self, Apr 25, 2024 4:00:00 PM
22. Chawki, M., Basu, S. and Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. Laws. [onlinel 13(3),p.33. doi:https://doi.org/10.3390/laws13030033.
23. Shahriar, H. (2024). Into the Metaverse: Technological Advances Shaping the Future of Consumer and Retail Marketing The Future of Consumption, pp.55-75. doi:https://doi.org/10.1007/978-3-031-33246-3 4.
24. Chohan, U.W. (2021). Non-fungible tokens: Blockchains, scarcity, and value. Critical Blockchain Research Initiative (CBRI) Working Papers
25. Hughes, L. (2023). Legal identity in the metaverse: Ownership, consent, and regulation. Journal of Virtual Law. 8(2), 45-59.
26. Kshetri, N. (2022). The emerging role of the metaverse in cybercrime. Computer, 55(8), 70-74. https://doi.org/10.1109/MC.2022.3169999
27. Terry, C. (2023). Challenges in policing the virtual world: Identity and jurisdiction in the metaverse. International Journal of Cybersecurity Law, 11(1), 23-37.
28. European Commission. (2018).General Data Protection Regulation (GDPR). https://gdpr.eu/ Interpol. (2023). 30.Cybercrime. https://www.interpol.int/en/Crimes/Cybercrime
29. Ministry of Electronics and Information Technology. (2023). Information Technology Act, 2000. Government of India. https://www.meity.gov.in