



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK
LEGAL

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer



Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and

a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has successfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of Law, Forensic Justice and Policy Studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Inter-country adoption laws from Uttarakhand University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat



Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University. More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.



Subhrajit Chanda



BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

BEYOND BORDERS: THE REGULATION OF VIRTUAL PROPERTY RIGHTS AND CRIMES IN THE METAVERSE

AUTHORED BY - VARSHINI R.K.¹

Abstract

The Metaverse—a network of immersive, persistent, and interconnected virtual environments—has emerged as a transformative frontier in the digital age, enabling social, economic, and cultural interactions beyond the confines of the physical world. With virtual real estate, Non-Fungible Tokens (NFTs), and decentralized economies gaining significant financial and social importance, the Metaverse presents complex legal challenges. Traditional doctrines of property, jurisdiction, and criminal liability, grounded in territorial sovereignty and physical presence, are ill-equipped to govern these borderless, decentralized, and pseudonymous interactions. This article critically examines the evolving legal landscape surrounding virtual property rights, NFTs, and virtual crimes, highlighting jurisdictional ambiguities, enforcement gaps, and conflicts between property and intellectual property law. It further evaluates the limitations of current national laws and regional frameworks, such as India's Information Technology Act, 2000, and the European Union's Digital Services and Markets Acts, in addressing cross-border digital disputes. The paper advocates for a hybrid regulatory framework that integrates international cooperation, platform accountability, technological safeguards, and ethical governance. Additionally, it emphasizes the importance of user education and digital literacy to empower participants in navigating virtual spaces responsibly. Ultimately, the article argues that law must evolve to recognize the tangible economic and social consequences of virtual activities, ensuring that rights, duties, and liabilities in the Metaverse are enforced with the same rigor as in the physical world, thereby fostering a secure, accountable, and sustainable digital ecosystem.

Keywords: *Metaverse, Virtual Property Rights, Non-Fungible Tokens (NFTs), Digital Assets, Jurisdiction, Cybercrime, Virtual Harms, Platform Governance, Blockchain Law, International Legal Harmonization, Digital Literacy.*

¹ Author: Varshini R.K., Practising Advocate, High Court of Madras,

I. Introduction

The Metaverse represents the next phase of the Internet—an immersive and interactive digital universe integrating augmented reality (AR), virtual reality (VR), blockchain technology, and artificial intelligence (AI). Unlike traditional online platforms, the Metaverse allows users to engage in social, economic, and cultural activities through avatars and digital identities. With virtual real estate sales crossing billions of dollars and NFTs functioning as proof of ownership, the Metaverse now supports an entire digital economy parallel to the physical world.²

However, the legal order has been slow to keep pace. Questions such as who owns virtual property, which nation's laws govern transactions between avatars, and how virtual crimes should be penalized challenge fundamental legal doctrines rooted in physical reality.³ Jurisdictional ambiguity, enforcement limitations, and lack of regulatory consistency create a vacuum that threatens the integrity of this new digital frontier.

II. Understanding the Metaverse and Its Legal Relevance

The term “Metaverse” was popularized by Neal Stephenson's *Snow Crash* (1992), depicting a shared virtual world inhabited by digital avatars. Today, it encompasses platforms like *Decentraland*, *The Sandbox*, *Roblox*, and *Meta's Horizon Worlds*. These spaces facilitate social interaction and commerce, creating new forms of digital ownership through blockchain verification.⁴

Legally, the Metaverse disrupts three foundational principles of law: territoriality, sovereignty, and identifiability. Traditional jurisdiction depends on physical territory, but virtual transactions transcend borders. Moreover, decentralized autonomous organizations (DAOs) and smart contracts reduce human control, complicating accountability.⁵ The result is a regulatory paradox—an environment that is economically tangible yet legally elusive.

²See Matthew Ball, *The Metaverse: And How It Will Revolutionize Everything* (2022).

³ Jack M. Balkin, “Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds,” 90 Va. L. Rev. 2043 (2004).

⁴ David J. Gunkel, *The Machine Question: Critical Perspectives on AI, Robots, and Ethics* (2012).

⁵ Lawrence Lessig, *Code and Other Laws of Cyberspace* 24–25 (1999).

III. Virtual Property Rights and NFTs

A. Defining Virtual Property

Virtual property includes digital assets such as avatars, virtual land, NFTs, and in-game goods. Although they have economic value, their legal characterization remains uncertain. In most jurisdictions, ownership of virtual property does not amount to real ownership but rather a contractual right governed by the platform's terms of service.⁶

For instance, purchasing a virtual land parcel in *Decentraland* via NFT does not necessarily confer full proprietary rights; instead, it provides a limited license subject to the platform's control.⁷ This discrepancy between perceived ownership and actual legal status raises critical questions about the enforceability of virtual transactions.

B. NFTs and Intellectual Property Conflicts

NFTs—unique blockchain-based tokens—serve as certificates of ownership for digital assets. However, owning an NFT does not automatically grant copyright over the underlying artwork or object.⁸ The *Hermès International v. Mason Rothschild* case (S.D.N.Y. 2023) illustrated this when the court held that the “MetaBirkin” NFTs violated Hermès' trademark rights.⁹ Similarly, *Nike v. StockX* highlighted the complexities of using NFTs for resale authentication without authorization.¹⁰

These cases reveal that NFT transactions often straddle the line between property and intellectual property law. Without clear legislative frameworks, users risk investing in assets with ambiguous or unenforceable rights.

IV. Jurisdictional Challenges in the Metaverse

A. The Limits of Territorial Jurisdiction

Legal jurisdiction traditionally depends on physical territory. Yet in the Metaverse, transactions occur in decentralized, non-physical environments. Determining the applicable law—whether based on the user's location, the platform's servers, or the blockchain's nodes—is complex.¹¹ Courts may invoke doctrines like the “effects test” (where the harm occurs) or minimum

⁶ Joshua A.T. Fairfield, “Virtual Property,” 85 B.U. L. Rev. 1047 (2005).

⁷ *Id.* at 1062.

⁸ Mike Ananny & Kate Crawford, “Seeing Without Knowing: Limitations of the Transparency Ideal,” 20 New Media & Soc'y 973 (2018).

⁹ *Hermès Int'l v. Rothschild*, No. 22-cv-384 (S.D.N.Y. 2023).

¹⁰ *Nike, Inc. v. StockX LLC*, No. 22-cv-983 (S.D.N.Y. 2023).

¹¹ Dan Svantesson, “A New Jurisprudential Framework for Jurisdiction,” 20 Yale J.L. & Tech. 105 (2018).

contacts (in U.S. law), but such principles strain under global, anonymous digital interactions.¹² For example, a fraud committed by a user in India on a victim in Germany through a U.S.-based virtual platform raises multi-jurisdictional conflict.

B. Emerging Models of Digital Jurisdiction

Some legal scholars propose “digital jurisdiction”, where the platform itself is treated as a quasi-sovereign entity with its own code-based governance.¹³ Others advocate for international treaties similar to the Budapest Convention on Cybercrime (2001), which harmonizes cross-border cooperation.¹⁴ However, such frameworks remain limited in scope and enforcement capability.

India’s Digital Personal Data Protection Act, 2023, and proposed amendments to the Information Technology Act, 2000, suggest a growing recognition of these challenges, but specific provisions for virtual assets are still absent.¹⁵

V. Crimes in the Metaverse: Virtual Harms and Real Liability

A. The Rise of Virtual Crimes

The Metaverse has already witnessed virtual harassment, fraud, and identity theft. Some incidents, such as sexual harassment of avatars, have raised concerns about psychological harm and digital consent.¹⁶ Similarly, virtual asset theft and phishing schemes exploit the lack of standard security and enforcement.

These offenses blur the line between virtual and real harm. Courts must decide whether harm to an avatar or virtual reputation constitutes a legally cognizable injury.¹⁷

B. Applying Existing Legal Frameworks

Existing cybercrime statutes can theoretically address Metaverse crimes. For instance, India’s Information Technology Act, 2000 criminalizes identity theft (Section 66C) and cyber fraud (Section 66D). Yet, enforcement is complicated by anonymity and cross-border data storage.¹⁸ The European Union’s Digital Services Act (2022) and Digital Markets Act (2022) represent early attempts at platform accountability. They require intermediaries to maintain transparent

¹² *Calder v. Jones*, 465 U.S. 783 (1984).

¹³ Andrew Murray, *Information Technology Law: The Law and Society* 238 (2019).

¹⁴ *Council of Europe Convention on Cybercrime* (Budapest, 2001).

¹⁵ *Digital Personal Data Protection Act, 2023* (India).

¹⁶ *BBC News*, “Meta Opens Investigation into Virtual Harassment in Horizon Worlds” (Feb. 2022)

¹⁷ *Balkin*, *supra* note 2, at 2050.

¹⁸ *Information Technology Act, 2000*, §§ 66C–66D (India).

governance and protect user rights.¹⁹ However, these are regional solutions to a global problem.

C. Evidence and Enforcement Challenges

Proving virtual crimes requires authenticating digital evidence—screenshots, blockchain transactions, and avatar activity logs. Chain-of-custody standards for such data remain underdeveloped.²⁰ Furthermore, anonymity tools and decentralized systems hinder identification of perpetrators.

Without mutual legal assistance treaties (MLATs) or standardized protocols, prosecuting Metaverse crimes remains largely aspirational.

VI. Towards a Regulatory Framework

A. Hybrid Governance Model

Given the limitations of traditional law, scholars suggest a hybrid regulatory framework combining:

1. **International Cooperation** – Developing multilateral treaties addressing virtual assets and crimes;
2. **Platform Self-Regulation** – Mandatory transparency, user rights protection, and due process; and
3. **Technological Regulation** – Embedding legal norms into code (“code is law”).²¹

This tripartite model balances innovation with accountability.

B. Role of Private Platforms

Platforms like *Meta*, *Decentraland*, and *Sandbox* effectively act as micro-sovereignities. They control economies, enforce rules, and adjudicate disputes internally.²² Hence, requiring them to adopt Digital Due Process Standards—including transparency, appeals, and audit mechanisms—may ensure fairness in governance.

C. The Path Toward International Norms

The long-term solution may lie in international digital law harmonization. The United Nations Commission on International Trade Law (UNCITRAL) could expand its remit to cover digital

¹⁹ *Digital Services Act*, Regulation (EU) 2022/2065; *Digital Markets Act*, Regulation (EU) 2022/1925.

²⁰ UNODC, *Practical Guide on Digital Evidence for Prosecutors* (2021).

²¹ *Lessig*, supra note 4, at 30.

²² *Fairfield*, supra note 5, at 1078.

property transactions and blockchain arbitration.²³ Likewise, the World Intellectual Property Organization (WIPO) might issue guidelines for NFT-related IP rights. Such institutional cooperation could bridge the legal vacuum between national laws and decentralized digital ecosystems.

VI. Policy Recommendations and Future Directions

The rapid expansion of the Metaverse presents a dual challenge: promoting innovation while ensuring accountability and legal certainty. Without proactive policy interventions, digital economies risk becoming hubs for exploitation, fraud, and unregulated activity. To address these concerns, several key policy measures and forward-looking strategies are necessary:

A. Strengthening User Protection and Digital Rights

First, regulators must prioritize safeguarding the rights of Metaverse participants. Users should enjoy clear, enforceable rights over digital assets, including the ability to transfer, sell, or collateralize NFTs and virtual property. Statutory recognition of digital assets as property is crucial to prevent arbitrary revocation by platforms.²⁴ Consumer protection laws should mandate transparency in terms of service, clear dispute resolution mechanisms, and redressal procedures for loss or theft of virtual assets. Additionally, users' privacy and data rights must be protected, particularly when immersive environments collect sensitive biometric or behavioral information. Comprehensive regulation could mandate encryption, consent-based data collection, and secure storage practices.

B. Integrating Ethics, Technology, and Law

The Metaverse is not purely economic; it is social and cultural. Therefore, ethical considerations must underpin legal frameworks. Legislators and platform developers should collaborate to define standards for acceptable behavior, consent, and harassment prevention. For instance, avatar-based harassment, "virtual sexual assault," and bullying have real psychological impacts. Legal recognition of such harms, combined with platform-level moderation and reporting mechanisms, is essential. Technology can assist in enforcement through smart contracts, automated monitoring, and algorithmic compliance systems, but these tools must be transparent and accountable to avoid bias or abuse.

²³ *UNCITRAL Secretariat*, "Possible Future Work on Digital Economy and Trade Law," U.N. Doc. A/CN.9/WG.IV/WP.167 (2023).

²⁴ *Digital Services Act*, Regulation (EU) 2022/2065; *Digital Markets Act*, Regulation (EU) 2022/1925.

C. Fostering International Cooperation

Given the Metaverse's inherently transnational nature, unilateral national regulation is insufficient. Policymakers should pursue international harmonization through treaties, model laws, and cross-border enforcement agreements. Organizations such as UNCITRAL, WIPO, and OECD can establish standards for virtual property recognition, dispute resolution, and cybersecurity compliance. Harmonization will reduce jurisdictional uncertainty, promote trust among users, and facilitate the resolution of cross-border disputes, including fraud, intellectual property violations, and asset recovery.

D. Preparing Legal Systems for Emerging Digital Economies

The legal system must evolve to recognize that economic value and harm are no longer confined to the physical world. Courts and regulators should adopt flexible doctrines capable of addressing virtual property, decentralized organizations, and novel financial instruments. Pilot programs, sandbox regulations, and specialized cyber tribunals may help courts and regulators test frameworks before nationwide implementation. Collaboration with technologists, economists, and ethicists will ensure that regulations balance innovation with accountability.

E. Promoting Awareness and Digital Literacy

Finally, education and awareness are critical. Users must understand the risks, rights, and responsibilities inherent in virtual environments. Platforms, regulators, and academic institutions should offer digital literacy programs, emphasizing secure transactions, identification of scams, and ethical participation. A well-informed user base strengthens the efficacy of regulation and reduces reliance on enforcement alone.

In sum, policy measures must be multi-layered—combining legal recognition, ethical guidance, technological enforcement, international harmonization, and user education. Such an integrated approach ensures that the Metaverse develops as a safe, accountable, and economically robust space while preserving its potential for innovation.

VII. Conclusion

The Metaverse represents a transformative frontier in the digital age, merging social, economic, and cultural interactions into immersive virtual environments that challenge traditional legal frameworks. Virtual property, including NFTs and digital real estate, carries tangible economic

value, while virtual crimes—ranging from fraud to harassment—can have real-world psychological and financial consequences. Yet, existing laws, anchored in physical territory and human-centric governance, are ill-equipped to address these borderless, decentralized, and pseudonymous interactions.

The analysis demonstrates that neither national legislation nor current international treaties can fully regulate virtual assets or adjudicate virtual crimes. Jurisdictional ambiguity, platform-centric governance, and decentralized technologies create enforcement gaps that could undermine trust in virtual economies if left unaddressed. To preserve both innovation and accountability, legal frameworks must evolve beyond traditional territorial concepts and integrate a multidimensional approach that blends international cooperation, platform regulation, technological safeguards, and ethical oversight.

Policy recommendations highlight the need for statutory recognition of digital assets, platform accountability through digital due process standards, international harmonization via treaties and model laws, and the embedding of legal norms into technology itself. Additionally, raising user awareness through digital literacy and ethical guidelines is essential to empower participants to navigate these virtual spaces responsibly.

Ultimately, the law's response to the Metaverse will define the balance between innovation and accountability in the digital economy. By adopting a hybrid governance model, legal systems can ensure that rights, duties, and liabilities in the virtual domain are treated with the same seriousness as in the physical world. Such an approach not only safeguards users and fosters trust but also positions the Metaverse as a sustainable and legally coherent ecosystem capable of supporting global innovation.