INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 4 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 4 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-4-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"EXTRA-TERRITORIAL APPLICATION OF CYBER LAWS: IS THE INFORMATION TECHNOLOGY ACT, 2000 ADEQUATE FOR METAVERSE CRIMES"

AUTHORS – PRAKHAR MISHRA* & DR KAVYA CHANDEL**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – PRAKHAR MISHRA & DR KAVYA CHANDEL "EXTRA-TERRITORIAL APPLICATION OF CYBER LAWS: IS THE INFORMATION TECHNOLOGY ACT, 2000 ADEQUATE FOR METAVERSE CRIMES", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 281-298, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The rapid emergence of the Metaverse as an immersive digital ecosystem has transformed the nature of online interaction, commerce, and identity. Powered by blockchain technology, non-fungible tokens (NFTs), cryptocurrencies, and augmented and virtual reality (AR/VR), virtual environments are evolving into complex socio-economic spaces where real-world legal consequences increasingly arise. However, the borderless architecture of these platforms presents unprecedented jurisdictional challenges for regulating cybercrime.

This dissertation examines the evolving problem of jurisdiction in Metaverse-related cybercrimes, with particular focus on the adequacy of existing legal frameworks to address offences committed in virtual realities. It explores the conceptual foundations of jurisdiction under international law, including territorial, nationality, protective, universality, and effects-based principles, and analyses their applicability to borderless digital platforms. The study further investigates the transformation of traditional cybercrimes into immersive offences such as avatar-based sexual harassment, NFT and cryptocurrency fraud, virtual property theft, identity cloning, and money laundering through digital assets.

Special emphasis is placed on the Indian legal framework, particularly the Information Technology Act, 2000 and relevant provisions of the Indian Penal Code, including the extra-territorial scope under Section 75. A comparative analysis of the regulatory approaches in the United States and the European Union highlights emerging models of digital governance and cross-border enforcement. The research identifies significant gaps in jurisdictional clarity, evidentiary standards, enforcement mechanisms, and recognition of virtual assets as legally protected property.

The study concludes that while existing cyber laws provide a foundational framework, they remain structurally insufficient to address the immersive, decentralized, and transnational nature of Metaverse crimes. It argues for a harmonised international regulatory model, clearer jurisdictional standards, strengthened platform accountability, and enhanced cross-border cooperation. Ultimately, the dissertation advocates for a forward-looking approach to cyber governance that reconciles digital innovation with effective legal accountability in virtual environments.

Keywords: Metaverse, Cybercrime, Jurisdiction, Extra-territoriality, Virtual Assets, Blockchain Governance, Digital Sovereignty, Cross-border Enforcement

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

INTRODUCTION

1.1 Background of the Study

Evolution from Cyberspace to the Metaverse

The development of the internet has undergone a transformative journey—from static web pages (Web 1.0) to interactive platforms (Web 2.0), and now toward decentralized and immersive ecosystems often described as Web 3.0. The latest phase of this evolution is the emergence of the "Metaverse[557]," a persistent, immersive, and interconnected virtual environment where users interact through avatars using technologies such as augmented reality (AR), virtual reality (VR), blockchain, and artificial intelligence.

Unlike traditional cyberspace, which primarily facilitated communication and information exchange, the Metaverse enables economic transactions, property ownership, social engagement, and even professional activities within virtual environments. Digital assets such as NFTs, cryptocurrencies, and virtual land have created parallel economies functioning beyond conventional territorial limitations.

This shift represents not merely technological advancement but a structural transformation of human interaction in digital space. Consequently, the legal challenges have expanded from regulating online content and cyber fraud to addressing crimes committed in immersive virtual realities, where physical presence is replaced by digital embodiment.

Rise of Immersive Digital Platforms

Major global corporations have invested heavily in immersive technologies, integrating virtual workspaces, digital marketplaces, and social hubs into interconnected virtual worlds. These platforms operate across jurisdictions, allowing users from different countries to interact simultaneously in a shared digital environment.

The rise of such immersive platforms has led to new forms of cybercrime, including:

- Avatar-based identity theft
- Virtual sexual harassment and assault
- Cryptocurrency and NFT fraud
- Theft or misappropriation of virtual assets
- Cross-border financial crimes

These offences often involve actors, victims, servers, and financial transactions located in multiple jurisdictions simultaneously. The traditional notion of "territory" becomes blurred, raising serious concerns regarding the applicability and enforcement of domestic cyber laws.

1.2 Statement of the Problem

Borderless Nature of the Metaverse

The Metaverse operates without geographical boundaries. A user in India may interact with a platform hosted in the United States, transact using cryptocurrency stored on decentralized blockchain networks, and engage with another user located in Europe—all within seconds. In such scenarios, determining:

- Where the crime was committed,
- Which country has jurisdiction, and
- Which law should apply becomes legally complex.

The principle of territorial sovereignty, which forms the foundation of criminal law, is challenged by the decentralized and transnational architecture of the Metaverse. Traditional jurisdictional rules are based on physical location—of the offender, victim, or harmful act. However, in immersive digital environments, these connecting factors are often dispersed or digitally obfuscated.

Extra-Territorial Application under the Information Technology Act, 2000

India addresses cross-border cyber offences through Section 75 of the Information Technology Act, 2000, which provides for extra-territorial application of the Act if the offence involves a computer, computer system, or

[557] *The Metaverse: And How It Will Revolutionize Everything* (Liveright Publishing, 2022).

computer network located in India[558]. While this provision appears broad, its practical adequacy in addressing Metaverse crimes remains uncertain. The Metaverse is built upon decentralized infrastructures, cloud computing systems, blockchain networks, and globally distributed servers. Identifying a clear "computer resource" nexus within Indian territory may not always be straightforward.

Further, issues such as:

- Attribution of digital identity to real-world individuals,
- Collection of digital evidence across borders,
- Cooperation with foreign jurisdictions, and
- Enforcement of judgments

pose significant practical obstacles.

Jurisdictional Uncertainty in Cross-Border Crimes

The jurisdictional uncertainty arises from:

1. Multiplicity of connecting factors (victim location, offender location, server location, blockchain nodes).
2. Anonymity and pseudonymity of avatars.
3. Decentralized architecture of blockchain-based assets.
4. Conflicts of laws between nations.

Although Section 75 attempts to extend India's jurisdiction beyond its territorial boundaries, questions remain as to whether it sufficiently addresses:

- Avatar-based crimes,
- Virtual property disputes,
- Crimes involving decentralized autonomous platforms,
- Transnational crypto-enabled fraud in immersive environments.

Thus, the central problem of this research is to examine[559] whether the existing extra-territorial framework under the IT Act, 2000 is legally and practically adequate to regulate emerging crimes in the Metaverse.

1.3 Research Objectives

1. To examine the concept and principles of extra-territorial jurisdiction in cyber law.
2. To analyze Section 75 of the Information Technology Act, 2000 and its scope.
3. To evaluate the applicability of the IT Act to Metaverse-based crimes.
4. To identify jurisdictional gaps in prosecuting cross-border immersive digital offences.
5. To suggest reforms for strengthening India's legal framework in addressing Metaverse cybercrimes.

1.4 Research Questions

1. What is the scope of extra-territorial jurisdiction under the Information Technology Act, 2000?
2. Can Section 75 effectively address crimes committed within decentralized and immersive Metaverse platforms?
3. What jurisdictional challenges arise in prosecuting cross-border Metaverse crimes?
4. Is the current Indian legal framework sufficient, or does it require legislative reform?
5. How can international cooperation mechanisms be strengthened to address jurisdictional conflicts?

1.5 Research Methodology

This research adopts a **doctrinal and analytical methodology**.

[558] NEAL STEPHONESON first introduced the concept of the Metaverse in the novel *Snow Crash*, where it was described as a persistent virtual environment accessed through digital avatars.

[559] *Principles of Cybercrime* (Cambridge University Press, 2nd ed., 2015).

- **Doctrinal Research:** Examination of statutory provisions, particularly the Information Technology Act, 2000, relevant amendments, and associated penal provisions.
- **Case Law Analysis:** Study of judicial interpretations relating to extra-territorial jurisdiction in cyber offences.
- **Comparative Analysis:** Evaluation of international approaches toward cross-border cyber jurisdiction.
- **Secondary Sources:** Review of scholarly articles, law commission reports, international conventions, and policy documents relating to cyber governance and digital sovereignty.

The research is qualitative in nature and focuses on identifying legal gaps, interpretative ambiguities, and enforcement challenges in the context of Metaverse crimes.

CONCEPTUAL FRAMEWORK: EXTRA-TERRITORIAL JURISDICTION IN CYBER LAW

2.1 Meaning and Scope of Extra-Territorial Jurisdiction

Jurisdiction refers to the legal authority of a State to prescribe, adjudicate, and enforce laws. Traditionally, criminal jurisdiction is territorially confined—States exercise authority over acts committed within their physical boundaries. However, globalization and digitalization have challenged this territorial paradigm, particularly in the context of cyber law.

Extra-territorial jurisdiction refers to the power of a State to apply its laws to conduct occurring outside its territorial boundaries, provided there exists a legally recognized connecting factor. In cyber law, such jurisdiction becomes crucial because digital activities frequently transcend national borders. A cyber offence may involve an offender in one country, a victim in another, servers in a third, and financial transactions routed through decentralized blockchain networks[560].

In India, Section 75 of the Information Technology Act, 2000 provides that the Act applies to offences committed outside India if the act involves a computer, computer system, or computer network located in India. This provision embodies extra-territorial jurisdiction based on a technological nexus.

The scope of extra-territorial jurisdiction in cyber law generally covers:

- Cross-border hacking and unauthorized access
- Online financial fraud
- Identity theft
- Data breaches affecting foreign citizens
- Digital asset crimes involving transnational transactions

However, its effectiveness depends upon:

1. Establishing a substantial connection between the offence and the regulating State.
2. Ensuring enforceability through international cooperation.
3. Harmonizing domestic laws with international legal principles.

In the context of the Metaverse, extra-territorial jurisdiction becomes more complex due to immersive technologies, decentralized infrastructures, avatar-based identities, and virtual property systems that operate without clear geographical anchors.

2.2 Principles of International Law Governing Jurisdiction

International law recognizes several principles that justify a State's assertion of jurisdiction beyond its borders. These principles provide the normative foundation for cyber jurisdiction.

[560] *International Law* (Cambridge University Press, 8th ed., 2017). The **territorial principle** allows states to exercise jurisdiction over acts committed within their territory.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A. Territorial Principle

The territorial principle is the primary and most universally accepted basis of jurisdiction. Under this principle, a State has authority over crimes committed within its physical territory. This principle has two dimensions:

- **Subjective territoriality** – jurisdiction over acts initiated within the State but completed elsewhere.
- **Objective territoriality** – jurisdiction over acts initiated outside the State but producing substantial effects within it.

In cyber law, territoriality becomes difficult to determine because digital acts lack physical boundaries. In the Metaverse, an avatar may commit harassment in a virtual environment hosted on a distributed server architecture, making it unclear where the offence "occurred." The absence of a physical situs challenges the applicability of classical territorial doctrine[561]. Nevertheless, States often rely on the objective territorial principle when the harmful impact is felt within their territory.

B. Nationality Principle

The nationality principle allows a State to exercise jurisdiction over its citizens regardless of where the offence is committed. This principle ensures that nationals remain accountable to their home State even for crimes committed abroad. In cybercrime cases, this principle may allow prosecution of:

- Indian citizens committing fraud on foreign platforms
- Nationals engaging in virtual asset scams through global Metaverse platforms

However, enforcement remains difficult when the accused resides outside the prosecuting State, particularly in the absence of extradition treaties or mutual legal assistance agreements. In immersive virtual spaces, identifying the real-world nationality behind an avatar presents evidentiary challenges due to pseudonymity and encryption.

C. Effects Doctrine

The effects doctrine permits a State to exercise jurisdiction when conduct outside its territory produces substantial and foreseeable effects within it.

This doctrine is particularly significant in cyber law. For example:

- A foreign hacker targeting Indian financial institutions
- A cross-border NFT fraud causing financial harm to Indian users
- Virtual harassment impacting Indian citizens psychologically or economically

The doctrine has been widely applied in digital contexts because it aligns with the borderless nature of online activities.

However, in the Metaverse, determining the "location" of effects becomes conceptually complex. Psychological harm, reputational damage, or economic loss may occur simultaneously across jurisdictions. Establishing a substantial and direct nexus is therefore legally intricate.

D. Protective Principle

Under the protective principle, a State may assert jurisdiction over acts committed outside its territory if such acts threaten its national security, sovereignty, or vital governmental interests.

In cyber law, this principle may justify jurisdiction over:

- Cyberterrorism in virtual platforms
- Attacks on national digital infrastructure
- Financial crimes affecting the national economy

In the Metaverse context, large-scale virtual financial manipulation, cryptocurrency laundering, or coordinated cyberattacks could invoke the protective principle.

[561] The **nationality principle** permits a state to regulate conduct of its nationals even when committed abroad.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

However, over-expansion of this principle may lead to jurisdictional conflicts and overlapping claims between States, potentially undermining international legal stability[562].

2.3 Jurisdictional Issues in Borderless Digital Platforms

The emergence of borderless digital platforms—and more recently, immersive Metaverse ecosystems—has created unprecedented jurisdictional challenges.

1. Multiplicity of Jurisdictional Claims

In a typical Metaverse crime scenario:

- The offender may reside in Country A.
- The victim may reside in Country B.
- The platform company may be incorporated in Country C.
- Servers may be distributed across multiple jurisdictions.
- Transactions may occur on decentralized blockchain nodes worldwide.

Each State may claim jurisdiction based on territoriality, nationality, or effects, leading to overlapping and conflicting legal claims.

2. Decentralization and Lack of Physical Anchors

Unlike traditional internet platforms with identifiable server locations, blockchain-based Metaverse platforms operate through decentralized nodes distributed globally. This decentralization weakens the traditional "server-location test"[563] often used to determine jurisdiction.

As a result:

- Identifying the situs of a virtual offence becomes ambiguous.
- Establishing territorial nexus becomes technically complex.
- Enforcement agencies face digital tracing challenges.

3. Anonymity and Avatar Identity

Metaverse interactions occur through avatars, which may not reflect real-world identities. Offenders may conceal nationality, residence, or physical location through:

- VPNs
- Encryption
- Decentralized identity systems

Without reliable attribution mechanisms[564], even asserting jurisdiction becomes procedurally challenging.

4. Enforcement and Mutual Legal Assistance Challenges

Even if jurisdiction is legally established, enforcement depends upon:

- Extradition treaties
- Mutual Legal Assistance Treaties (MLATs)
- International cybercrime conventions

Delays, bureaucratic hurdles, and political considerations[565] often obstruct effective cross-border prosecution.

5. Conflict of Laws

Different jurisdictions may:

- Criminalize certain virtual conduct differently,
- Apply varying standards of intermediary liability,
- Have divergent evidentiary rules,
- Regulate digital assets inconsistently.

This divergence results in regulatory fragmentation[566], allowing offenders to exploit "jurisdictional safe havens."

[562] The **protective principle** allows jurisdiction over acts threatening national security or governmental interests.

[563] The **universality principle** permits prosecution of universally condemned crimes regardless of where they occur.

[564] The **universality principle** permits prosecution of universally condemned crimes regardless of where they occur.

[565] "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* (1996).

[566] *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, 2006).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

LEGAL FRAMEWORK UNDER THE INFORMATION TECHNOLOGY ACT, 2000

3.1 Objectives and Scope of the Act

The Information Technology Act, 2000 (IT Act) was enacted to provide legal recognition to electronic transactions, facilitate e-commerce, and address cyber offences in India[567]. It marked India's first comprehensive attempt to regulate activities in cyberspace.

The primary objectives of the Act include:

- Legal recognition of electronic records and digital signatures.
- Facilitation of electronic governance and online transactions.
- Prevention and punishment of cyber offences.
- Protection of data integrity and digital infrastructure.

Over time, particularly through the 2008 amendment, the Act expanded its penal framework to include offences such as identity theft, cyber fraud, privacy violations, and cyber terrorism. However, the Act was originally designed to regulate traditional internet-based crimes rather than immersive virtual environments like the Metaverse.

Scope of the Act

The Act applies to:

- Offences involving a "computer," "computer system," or "computer network."
- Digital transactions and electronic records.
- Intermediary liability and due diligence obligations.

In the context of the Metaverse, the applicability of the Act depends on whether immersive virtual interactions fall within the statutory definitions of "computer resource" under Section 2(1)(k). Since Metaverse platforms operate through interconnected computer networks and digital systems, they technically fall within the Act's scope. However, challenges arise in applying traditional cybercrime provisions to avatar-based, blockchain-driven, and decentralized platforms.

3.2 Section 75: Extra-Territorial Application

Text of Section 75

Section 75(1) of the IT Act provides that:

The Act applies to any offence or contravention committed outside India by any person, irrespective of nationality, if the act or conduct constituting the offence involves a computer, computer system, or computer network located in India.

Section 75(2) further clarifies that this provision shall apply even if the offender is located outside India.

Interpretation

Section 75 establishes extra-territorial jurisdiction based on a technological nexus rather than physical presence. The essential requirement is the involvement of a "computer resource" located in India.

This means:

- A foreign national committing a cyber offence[568] targeting an Indian server may be prosecuted under Indian law.
- A cross-border digital fraud affecting Indian computer networks may fall within Indian jurisdiction.

However, interpretation issues arise in the context of the Metaverse:

1. **Decentralized Infrastructure** – Many Metaverse platforms operate on cloud-based or blockchain networks distributed globally. Identifying a specific "computer resource located in India" may be difficult.

[567] Cybercrimes in virtual environments may include harassment, identity theft, and financial fraud conducted through avatars.

[568] Bitcoin and other digital currencies facilitate financial transactions in decentralized virtual environments.

2. **Virtual Transactions** – NFT or cryptocurrency-based offences may occur on decentralized ledgers without a clearly identifiable territorial server.
3. **Data Localization Ambiguity** – If data is mirrored or stored in multiple jurisdictions, determining whether Section 75 is triggered becomes legally complex.

Thus, while Section 75 provides a statutory basis for extra-territorial jurisdiction, its practical applicability to immersive and decentralized environments remains uncertain.

Judicial Understanding

Indian courts have recognized extra-territorial jurisdiction in cyber offences where a sufficient nexus to India exists. For instance, in **Sharat Babu Digumarti v. Government (NCT of Delhi)**, the Supreme Court clarified the relationship between offences under the IT Act and the IPC, emphasizing the special nature of cyber offences. Although the case did not directly interpret Section 75 in a Metaverse context, it reinforced that cyber offences must be prosecuted within the framework of the IT Act where applicable.

Judicial practice generally requires:

- A demonstrable connection to Indian computer systems,
- Evidence of harm or impact within India,
- Compliance with procedural safeguards under criminal law.

However, there is limited jurisprudence directly addressing Metaverse-specific crimes, indicating a developing area of law.

3.3 Relevant Penal Provisions Applicable to Metaverse Crimes

Although the IT Act predates the Metaverse, several penal provisions may apply to offences committed within immersive virtual environments.

A. Identity Theft – Section 66C

Section 66C criminalizes fraudulent or dishonest use of electronic signatures, passwords, or unique identification features.

In the Metaverse[569] context, this provision may apply to:

- Unauthorized access to another user's avatar account.
- Theft of login credentials to transfer virtual assets.
- Impersonation using stolen digital identity credentials.

Since avatars represent digital identities linked to user accounts, unauthorized access or misuse can fall within the ambit of identity theft.

B. Cheating by Personation – Section 66D

Section 66D penalizes cheating by personation through computer resources.

This provision becomes highly relevant in Metaverse scenarios involving:

- Fake investment schemes involving virtual land or NFTs.
- Fraudulent crypto-wallet transactions.
- Avatar-based impersonation for financial gain.

If a user creates a false digital persona to deceive another user into transferring cryptocurrency or virtual assets, Section 66D may be invoked. However, cross-border enforcement remains challenging when the perpetrator operates from outside India.

C. Privacy Violations – Section 66E

Section 66E criminalizes the intentional capture, publication, or transmission of images of private areas without consent. In immersive virtual platforms where VR devices collect biometric and behavioral data, privacy concerns extend beyond traditional image-based violations. Issues may include:

[569] *Navigating the Metaverse: A Guide to Legal and Governance Issues* (2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

- Unauthorized recording of immersive interactions.
- Capture of biometric data (eye tracking, facial mapping).
- Non-consensual sharing of virtual intimate experiences.

Although Section 66E primarily addresses physical privacy, its principles may be extended to certain forms of digital privacy violations within the Metaverse.

3.4 Interplay with the Indian Penal Code

The IT Act does not function in isolation. Cyber offences often overlap with provisions of the Indian Penal Code, 1860 (IPC).

Relevant IPC provisions include:

- Section 419 – Cheating by personation.
- Section 420 – Cheating and dishonestly inducing delivery of property.
- Section 354A – Sexual harassment (applicable in certain virtual harassment scenarios).
- Section 499 – Defamation.

The Supreme Court in **Sharat Babu Digumarti v. Government (NCT of Delhi)** clarified that where a special law (like the IT Act) specifically covers an offence, prosecution should primarily proceed under that special statute rather than the IPC, following the principle of *generalia specialibus non derogant*. However, in cases where:

- The IT Act lacks specific provisions (e.g., virtual sexual assault without physical contact), or
- The offence involves elements beyond digital misuse (e.g., criminal intimidation combined with cyber threats), the IPC[570] may supplement the IT Act.

Challenges in Interplay

1. Overlapping offences may create ambiguity in charge framing.
2. Certain Metaverse crimes lack explicit statutory recognition under both laws.
3. Virtual property rights are not clearly defined under existing penal provisions.

Thus, while the IT Act and IPC[571] collectively provide a framework to prosecute certain Metaverse offences, significant doctrinal and practical gaps remain.

ADEQUACY ANALYSIS – IS SECTION 75 SUFFICIENT FOR METAVERSE CRIMES? (CRITICAL EVALUATION SECTION)

Adequacy of the Information Technology Act, 2000 in Addressing Metaverse Crimes

The rapid evolution of immersive digital ecosystems has fundamentally altered the nature of cybercrime. While the Information Technology Act, 2000 (IT Act)[572] provides a statutory framework for cyber offences, its adequacy in addressing crimes emerging within the Metaverse requires critical examination.

4.1 Nature of Metaverse Crimes.

The Metaverse differs from traditional cyberspace in three key ways:

1. Immersive, embodied interactions through avatars

2. Digital ownership of virtual assets

3. Integration of blockchain-based economies

These characteristics give rise to unique categories of offences.

A. Avatar-Based Offences

In the Metaverse, users operate through avatars that represent their digital identities. Crimes committed through avatars may include:

[570] Intellectual property concerns arise where digital assets and NFTs replicate copyrighted works without authorization.

[571] Evidence in virtual crimes may involve digital logs, blockchain transaction records, and platform metadata.

[572] provides the primary framework for cybercrime regulation in India.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- **Impersonation**
- **Harassment**
- **Defamation**
- **Fraudulent misrepresentation**

While Sections 66C and 66D of the IT Act may address identity theft and personation, the immersive and behavioral dimension of avatar-based misconduct presents conceptual challenges. For example, non-consensual virtual touching or simulated assault raises questions about psychological harm and legal recognition of "virtual bodily autonomy," which the Act does not explicitly contemplate.

B. Virtual Property Theft : Virtual land, in-game assets, and blockchain-based collectibles hold real-world economic value. Theft or unauthorized transfer of such assets may not neatly fit within traditional definitions of movable property under criminal law. The IT Act addresses unauthorized access and data theft, but it does not clearly define virtual property rights. Where blockchain tokens or NFTs are stolen, prosecution may rely on identity theft or cheating provisions rather than a clear statutory recognition of digital asset misappropriation.

This creates doctrinal ambiguity regarding:

- Whether virtual assets constitute "property" under Indian criminal law,
- How ownership is legally established, and
- Which jurisdiction applies when blockchain nodes are globally distributed.

C. NFT and Cryptocurrency Fraud: NFT scams, rug pulls, phishing schemes, and crypto-wallet thefts are increasingly common in immersive platforms. Such offences may involve:

- Cross-border financial transfers
- Decentralized exchanges
- Smart contracts

Although the IT Act penalizes computer-related fraud, it does not specifically regulate blockchain ecosystems. The absence of comprehensive cryptocurrency regulation in India further complicates enforcement.

D. Virtual Sexual Harassment:

One of the most debated issues in the Metaverse is virtual sexual harassment or assault. Immersive VR environments allow users to experience simulated physical proximity and interaction. While Section 66E of the IT Act addresses privacy violations and the Indian Penal Code, 1860[573] criminalizes sexual harassment under Section 354A, both laws are grounded in physical-world assumptions.

Key legal questions include:

- Can virtual touching constitute actionable harm?
- Does psychological trauma in immersive environments meet legal thresholds?
- How is jurisdiction determined when parties are located in different countries?

The IT Act does not explicitly address these emerging harms.

4.2 Enforcement Challenges

Even if statutory provisions appear applicable, enforcement in Metaverse crimes presents significant obstacles.

The issue of jurisdiction in metaverse-related cybercrimes is deeply intertwined with challenges of identity attribution, cross-border investigation, and digital evidence collection. In virtual environments, users frequently operate through pseudonymous avatars, while blockchain-based systems reinforce anonymity through cryptographic keys, making it difficult to link digital wallets and virtual identities to real individuals. The use of VPNs, proxy servers, and privacy-enhancing technologies further complicates efforts to trace offenders, particularly when crimes transcend territorial boundaries. Metaverse offences often involve offenders located in one jurisdiction, victims in another, platform operators in a third, and decentralized technological infrastructure spread across multiple States. Such complexity

[573] provisions relating to cheating, fraud, and identity theft may apply to digital offences.

necessitates reliance on mechanisms such as Mutual Legal Assistance Treaties (MLATs), extradition agreements, and international cybercrime conventions; however, procedural delays, jurisdictional conflicts, and lack of harmonized legal standards significantly hinder timely and effective prosecution. Additionally, evidence in immersive platforms may include VR interaction logs, blockchain transaction histories, avatar communication data, and biometric tracking records. The preservation, authentication, and admissibility of such digital evidence raise serious concerns relating to chain of custody, data localization requirements, and evidentiary standards. Notably, the Information Technology Act, 2000 does not provide detailed procedural mechanisms specifically tailored to immersive digital environments, thereby creating regulatory and enforcement gaps despite the existence of substantive penal provisions.

4.3 Limitations of Section 75: Section 75 of the IT Act extends the Act's application beyond India's territorial boundaries, provided the offence involves a computer resource located in India.

A. Requirement of "Computer Resource" Nexus : The provision requires a nexus to a computer, system, or network located within India. In decentralized Metaverse environments:

- Servers may be cloud-based and geographically dispersed.
- Blockchain nodes operate across jurisdictions simultaneously.
- Data storage may be fragmented.

Establishing a clear Indian nexus becomes technically complex. If no identifiable server or infrastructure is located in India, asserting jurisdiction under Section 75 may be legally contested.

B. Practical Enforcement Barriers: Even when jurisdiction is established:

- Foreign accused persons may not be extradited.
- Foreign platform companies may resist compliance.
- Decentralized autonomous organizations (DAOs) may lack a legal personality to prosecute.

Thus, Section 75 provides theoretical jurisdiction but limited practical enforceability.

4.4 Comparative Perspective: A comparative analysis demonstrates how other jurisdictions address extra-territorial cyber regulation.

A. U.S. Approach to Extra-Territorial Cyber Jurisdiction: The United States[574] adopts a broad interpretation of extra-territorial jurisdiction, often relying on:

- The effects doctrine
- Federal statutes with explicit extra-territorial clauses
- Aggressive enforcement mechanisms

The Computer Fraud and Abuse Act (CFAA) and federal wire fraud statutes have been applied to cross-border cyber offences where U.S. interests are affected. U.S. courts frequently assert jurisdiction if:

- The victim is located in the U.S.,
- U.S. financial systems are involved, or
- Substantial effects occur within U.S. territory.

The U.S. also actively uses international cooperation and extradition treaties, enhancing enforcement effectiveness.

B. European Union Digital Governance Framework: The European Union emphasizes regulatory harmonization and data protection. The EU framework relies on:

- General Data Protection Regulation (GDPR)[575] extra-territorial reach
- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- The GDPR applies to entities outside the EU if they process data of EU residents. This effects-based jurisdiction model

[574] The **United States** applies jurisdiction in cyber cases through principles such as the **effects doctrine**.
[575] The General Data Protection Regulation provides extra-territorial application to protect digital data of EU citizens.

provides stronger cross-border[576] regulatory authority.

The EU also promotes coordinated enforcement among Member States, reducing fragmentation.

Critical Evaluation: Compared to the U.S. and EU:

- India's IT Act provides extra-territorial jurisdiction but lacks detailed enforcement mechanisms. It does not comprehensively regulate blockchain, NFTs, or immersive harms. It relies heavily on a territorial nexus that may be outdated in decentralized ecosystems. Thus, while the IT Act lays a foundational framework, it is not fully adequate to address the complex, decentralized, and immersive nature of Metaverse crimes.

FINDINGS AND RECOMMENDATIONS

5.1 Major Findings of the Study

The analysis of the Information Technology Act, 2000 in the context of Metaverse crimes reveals several structural[577] and doctrinal gaps.

1. The IT Act Was Not Designed for Immersive Digital Ecosystems

The Act was enacted at a time when cyberspace primarily involved email communication, website-based transactions, and basic online fraud. It does not contemplate:

- Avatar-based embodied interactions
- Blockchain-based ownership models
- Decentralized autonomous platforms
- Immersive virtual harms

As a result, its provisions apply indirectly rather than specifically to Metaverse offences.

2. Section 75 Provides Theoretical but Limited Practical Extra-Territorial Jurisdiction

Section 75 extends jurisdiction where a "computer resource" in India is involved. However:

- Decentralized blockchain systems lack clear territorial anchoring.
- Cloud-based infrastructure complicates identification of server location.
- Many Metaverse platforms operate globally without fixed data localization.

Thus, while jurisdiction may exist in theory, proving the required nexus is technologically and evidentially challenging.

3. Enforcement Mechanisms Are Weak in Cross-Border Contexts

The primary barriers are:

- Attribution of anonymous avatars
- Limited international cooperation
- Delays in mutual legal assistance processes
- Absence of harmonized cybercrime standards

Without effective enforcement, extra-territorial jurisdiction remains largely symbolic.

4. Virtual Property and Immersive Harm Lack Clear Legal Recognition

The Act does not explicitly define:

- Virtual assets as legally protected property
- Avatar identity as a legally safeguarded digital personality
- Immersive psychological harm as a prosecutable injury

This creates uncertainty in prosecuting NFT theft, virtual land fraud, and virtual sexual misconduct.

Comparative Jurisdictions Adopt More Dynamic Approaches: The United States relies heavily on the effects doctrine and strong

[576] Cross-border cyber investigations often require mutual legal assistance treaties and international cooperation mechanisms.
[577] Jurisdictional ambiguity remains one of the primary legal challenges in regulating crimes occurring within decentralized virtual environments.

enforcement mechanisms. The European Union uses regulatory extraterritoriality under frameworks like GDPR and coordinated enforcement models. India's framework, by contrast, remains infrastructure-dependent and territorially anchored[578].

5.2 Critical Gaps Identified

The research identifies five primary gaps:

1. **Outdated territorial nexus requirement** in Section 75.
2. **Absence of metaverse-specific definitions and offences.**
3. **No comprehensive regulation of blockchain and NFTs.**
4. **Weak cross-border enforcement mechanisms.**
5. **Lack of international digital cooperation treaties specifically addressing immersive platforms.**

5.3 Recommendations

1. Clarification and Expansion of Extra-Territorial Jurisdiction

Section 75 should be amended to:

- Incorporate an explicit **effects-based jurisdiction model**, allowing prosecution where substantial harm occurs in India, regardless of server location.
- Recognize decentralized digital infrastructures and blockchain systems.

2. Introduction of Metaverse-Specific Provisions

The IT Act should be amended to include:

- Legal recognition of virtual assets as protected digital property.
- Specific offences for avatar-based harassment and immersive abuse.
- Clear standards for digital identity protection in immersive environments.

This would reduce reliance on indirect application of traditional cybercrime provisions.

3. Regulation of Blockchain and Digital Asset Ecosystems

A comprehensive regulatory framework for NFTs and cryptocurrency transactions should:

- Define ownership rights.
- Establish fraud prevention standards.
- Impose due diligence obligations on platform operators.

This would strengthen accountability within Metaverse economies.

4. Strengthening International Cooperation

India should:

- Enhance Mutual Legal Assistance Treaty (MLAT) efficiency.
- Participate actively in global cybercrime conventions.
- Advocate for a multilateral framework addressing jurisdiction in virtual realities.

Since Metaverse platforms are inherently global, unilateral regulation is insufficient.

5. Development of Specialized Cyber Enforcement Units

Given the technical complexity of immersive crimes, law enforcement agencies must:

- Develop blockchain forensic capabilities.
- Establish digital evidence preservation protocols.
- Train officers in immersive technology investigation.

5.4 Proposed Model for Future Regulation

A hybrid jurisdictional model is recommended:

1. **Effects-based jurisdiction** (harm-focused).
2. **Platform accountability regime** (intermediary obligations).
3. **International harmonization of cybercrime standards.**

[578][578] International cooperation through organizations such as the United Nations and the INTERPOL is essential for effective enforcement.

4. **Digital sovereignty safeguards balanced with global cooperation.**

Such a model would reconcile territorial sovereignty with borderless digital realities.

5.5 Concluding Observations

The research concludes that while the Information Technology Act, 2000 provides a foundational legal structure and includes extra-territorial provisions under Section 75, it is not fully adequate to regulate Metaverse[579] crimes effectively.

The immersive, decentralized, and transnational nature of virtual realities exposes significant limitations in:

- Territorial nexus requirements
- Attribution standards
- Enforcement capacity
- Legal recognition of digital harms

Therefore, legislative reform, doctrinal evolution, and international collaboration are essential to ensure that cyber law remains responsive to the realities of the Metavers

RECOMMENDATIONS AND WAY FORWARD

The evolution of immersive virtual environments demands a forward-looking regulatory response. While the Information Technology Act, 2000 provides a foundational cyber law framework, it requires doctrinal clarification and structural reform to address jurisdictional and enforcement challenges in the Metaverse.

6.1 Clarification of Jurisdictional Standards

One of the most pressing concerns in regulating Metaverse crimes is ambiguity in jurisdictional standards. Section 75 of the IT Act predicates extra-territorial application on the involvement of a "computer resource" located in India. However, decentralized cloud architecture and blockchain-based systems dilute the clarity of territorial nexus. To address this, the following reforms are recommended:

1. Adoption of an Effects-Based Jurisdiction Model

The law should explicitly incorporate an "effects doctrine" approach, allowing Indian courts to exercise jurisdiction where:

- Substantial harm is caused to Indian citizens,
- Financial loss occurs within Indian territory, or
- Indian digital sovereignty is impacted.

This would reduce over-reliance on server-location tests and align India's framework with global regulatory trends.

2. Defining Digital Nexus Standards

Clear statutory guidelines should be introduced to determine:

- When digital infrastructure constitutes sufficient territorial connection,
- Whether cloud mirroring or distributed servers qualify as Indian nexus,
- How blockchain nodes should be treated for jurisdictional purposes.

Clarity would enhance predictability and reduce litigation ambiguity.

6.2 Need for Metaverse-Specific Provisions

The IT Act was enacted in 2000—long before immersive digital realities emerged. While certain provisions indirectly apply, the absence of Metaverse-specific recognition limits prosecutorial clarity.

1. Recognition of Virtual Assets as Legal Property

Legislation should define:

- NFTs, virtual land, and digital collectibles as legally protectable property,
- Ownership standards for blockchain-based assets,
- Criminal liability for unauthorized transfer or misappropriation.

[579] Harmonised global regulatory frameworks are necessary to address emerging digital environments such as the Metaverse.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

This would eliminate doctrinal uncertainty in prosecuting virtual property theft.

2. Criminalization of Immersive Harms

Specific provisions should address:

- Avatar-based harassment and simulated assault,
- Non-consensual immersive interactions,
- Biometric and behavioral data exploitation.

As immersive technologies replicate physical experiences, legal frameworks must acknowledge psychological and reputational harm occurring in virtual environments.

3. Enhanced Intermediary Accountability

Metaverse platforms should be subject to:

- Stronger due diligence obligations,
- Transparency requirements regarding data processing and user identity verification,
- Compliance mechanisms for cross-border law enforcement requests.

Platform governance must evolve alongside technological complexity.

6.3 Strengthening International Cooperation

Metaverse crimes are inherently transnational. Domestic legislation alone cannot ensure effective enforcement.

1. Streamlining Mutual Legal Assistance Mechanisms

India should reform procedural delays in MLAT processes by:

- Digitizing request systems,
- Establishing fast-track cybercrime cooperation cells,
- Creating standardized digital evidence exchange protocols.

Timely cooperation is crucial in blockchain-based offences where funds may be rapidly transferred.

2. Participation in Global Cybercrime Conventions

India should actively engage in multilateral cybercrime initiatives and advocate for updated international instruments that specifically address immersive technologies.

Global coordination would:

- Minimize jurisdictional conflicts,
- Prevent regulatory safe havens,
- Promote harmonized enforcement standards.

3. Cross-Border Data Governance Agreements: Bilateral and regional agreements on:

- Data sharing,
- Evidence preservation,
- Blockchain tracing collaboration

would significantly strengthen extra-territorial enforcement capacity.

6.4 Proposal for a Harmonised Global Framework: Given the borderless nature of virtual realities, a fragmented national approach is insufficient. A harmonised global framework is essential.

Core Elements of the Proposed Framework

1. **Uniform Definition of Metaverse Crimes**: Establish internationally accepted definitions for avatar-based offences, digital asset theft, and immersive harassment.
2. **Standardized Jurisdictional Principles**: Combine territoriality, nationality, and effects-based approaches into a hybrid jurisdiction model applicable to immersive platforms.
3. **Platform Responsibility Charter**: Impose global compliance standards on Metaverse companies, including:
    - Identity verification protocols,
    - Transparent governance policies,

- Cooperation with law enforcement agencies.

4. **Digital Evidence and Forensics Protocols**: Develop uniform evidentiary standards for:
    - Blockchain tracing,
    - VR interaction logs,
    - Biometric data handling.

Balancing Digital Sovereignty and Global Governance

While harmonization is necessary, States must preserve digital sovereignty. The proposed model should:

- Respect national constitutional principles,
- Prevent overreach by foreign authorities,
- Ensure protection of user privacy and fundamental rights.

Thus, the future of cyber jurisdiction lies in cooperative sovereignty rather than isolated territorial regulation. The adequacy of the IT Act in addressing Metaverse crimes is limited not due to absence of intent but due to technological transformation outpacing legislative design. Clarifying jurisdictional standards, introducing Metaverse-specific provisions, strengthening international cooperation, and advocating for a harmonised global framework are essential steps toward effective governance of virtual realities.

Without proactive reform, jurisdictional uncertainty will continue to undermine accountability in the rapidly expanding Metaverse ecosystem.

Conclusion

Summary of Arguments

This research examined the question: *Is the extra-territorial framework under the* Information Technology Act, 2000 *adequate to address crimes committed within the Metaverse?*

The study began by situating the Metaverse within the broader evolution of cyberspace—highlighting how immersive virtual environments, blockchain-based economies, NFTs, and avatar-driven interactions have fundamentally transformed the nature of digital engagement. Unlike traditional cybercrime, Metaverse offences involve embodied digital identities, virtual property rights, and psychologically immersive harm.

The conceptual analysis demonstrated that extra-territorial jurisdiction in cyber law rests upon established principles of international law: territoriality, nationality, the effects doctrine, and the protective principle. However, the borderless architecture of immersive platforms challenges the practical application of these doctrines. Distributed servers, decentralized blockchain networks, and anonymous digital identities dilute traditional notions of territorial nexus.

The examination of Section 75 of the IT Act revealed that while India has legislatively recognized extra-territorial applicability, its framework is conditional upon the involvement of a "computer resource" located in India. This creates ambiguity in cases involving cloud computing, decentralized systems, and cross-border immersive interactions. Although certain provisions—such as Sections 66C, 66D, and 66E—can be applied to identity theft, online impersonation, and privacy violations in virtual environments, the Act lacks explicit recognition of virtual property, avatar-based harm, and blockchain-related fraud.

Comparative analysis further illustrated that jurisdictions such as the United States and the European Union have increasingly adopted effects-based approaches and stronger digital governance models, thereby expanding regulatory reach in transnational cybercrime cases. India's framework, while foundational, remains reactive rather than anticipatory in addressing immersive digital realities.

Final Answer to the Research Question

The central research question asked whether the extra-territorial application of the IT Act,

2000 is adequate to regulate Metaverse crimes. The answer is **partially but not fully**.

The Act provides a jurisdictional basis through Section 75 and contains penal provisions adaptable to certain Metaverse-related offences. However, its adequacy is limited by:

- Ambiguity in establishing territorial nexus in decentralized environments,
- Absence of clear statutory recognition of virtual assets and immersive harms,
- Practical enforcement barriers in cross-border investigations,
- Heavy reliance on traditional concepts of "computer resource" rather than digital impact or effects.

Thus, while the IT Act offers a starting point, it is structurally insufficient to comprehensively address the complex jurisdictional realities of immersive virtual ecosystems. Legislative clarification, doctrinal evolution, and international cooperation are essential to bridge this gap.

Future Implications for Cyber Governance

The rise of the Metaverse signals a broader transformation in cyber governance. Digital spaces are no longer mere communication platforms; they are emerging socio-economic ecosystems with tangible financial, psychological, and legal consequences.

Future cyber governance must therefore:

1. **Adopt Hybrid Jurisdiction Models**: Moving beyond rigid territoriality toward integrated territorial, nationality, and effects-based approaches.
2. **Recognize Virtual Rights and Assets**: Legal systems must evolve to treat digital identities and virtual property as legally protected interests.
3. **Strengthen Global Regulatory Cooperation**: As immersive platforms operate across jurisdictions, harmonized international standards will become indispensable.
4. **Balance Innovation with Accountability**: Over-regulation may stifle technological development, while under-regulation risks creating digital safe havens for criminality. A calibrated, rights-respecting framework is essential.

Ultimately, the future of Metaverse governance will depend on whether legal systems can transition from reactive cyber regulation to proactive digital constitutionalism. The challenge is not merely technological but jurisprudential: redefining jurisdiction in a world where reality itself is increasingly virtual.

Bibliography

A. Books

1. Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd ed., 2015).
2. Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger Publishers, 2010).
3. Brian Craig, *Cyberlaw: The Law of the Internet and Information Technology* (Pearson Education, 2013).
4. Chris Reed & John Angel, *Computer Law* (Oxford University Press, 8th ed., 2018).
5. Yatindra Singh, *Cyber Laws* (Universal Law Publishing, 2017).
6. Pavan Duggal, *Cyberlaw: The Indian Perspective* (Saakshar Law Publications, 2014).

B. Journal Articles

1. David R. Johnson & David Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* (1996).
2. Jack L. Goldsmith & Tim Wu, "The Internet and the Sovereign State," *Harvard Law Review* (2006).
3. "Cybercrime Prosecution in the Metaverse: Evidentiary and Jurisdictional Challenges," *Journal of Law and Social Development* (2023).

4. "Legal Framework for Cybersecurity in the Context of the Metaverse Formation," *Modern Studies in Social Law* (2022).
5. "Identity, Crimes and Law Enforcement in the Metaverse," *Humanities and Social Sciences Communications* (2024).
6. "Consumer Protection in Blockchain-Based Metaverses," *Frontiers in Blockchain* (2025).

C. Reports and Policy Documents

1. Law Commission of India, *Report on Cybercrime and Digital Evidence*.
2. NITI Aayog, *Blockchain: The India Strategy Report* (2020).
3. World Economic Forum, *Navigating the Metaverse: Governance and Legal Challenges* (2023).
4. Organisation for Economic Co-operation and Development, *Policy Framework for Digital Security* (2021).

D. Legislation

1. Information Technology Act, 2000.
2. Indian Penal Code.
3. Digital Personal Data Protection Act, 2023.
4. General Data Protection Regulation.

E. Online Sources

1. CERT-In – https://www.cert-in.org.in
2. United Nations Office on Drugs and Crime Cybercrime Repository – https://www.unodc.org
3. European Commission Digital Strategy – https://digital-strategy.ec.europa.eu
4. World Intellectual Property Organization Digital Property and Blockchain Resources – https://www.wipo.int