

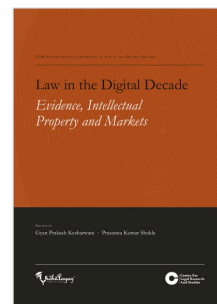
CHAPTER 8

Cybercrime in the Metaverse: Identity, Jurisdiction and Digital Evidence

Rupali Mehta and Ashwini Yadav

in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 69–82

DOI <https://doi.org/10.63108/VAB.LDD.2.8>



CITATIONS

BLUEBOOK (21ST ED.)

Rupali Mehta & Ashwini Yadav, *Cybercrime in the Metaverse: Identity, Jurisdiction and Digital Evidence*, in *LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS* 69 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Rupali Mehta and Ashwini Yadav, 'Cybercrime in the Metaverse: Identity, Jurisdiction and Digital Evidence' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 69.

CHICAGO (17TH ED.)

Mehta, Rupali, and Ashwini Yadav. "Cybercrime in the Metaverse: Identity, Jurisdiction and Digital Evidence." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 69–82. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.2.8>.

APA (7TH ED.)

Mehta, R., & Yadav, A. (2026). Cybercrime in the metaverse: Identity, jurisdiction and digital evidence. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 69–82). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.2.8>

SOURCE

<https://doi.org/10.63108/VAB.LDD.2.8>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 8

Cybercrime in the Metaverse: Identity, Jurisdiction and Digital Evidence

RUPALI MEHTA* AND ASHWINI YADAV**

The metaverse is emerging as a network of persistent, immersive and economically active digital environments in which people communicate through avatars, acquire virtual assets and generate continuous streams of behavioural and biometric data. The same architecture that produces presence and interoperability also enlarges the opportunity structure for crime. Identity theft may become avatar takeover or biometric mimicry; fraud may be executed through smart contracts and virtual goods; harassment may be embodied and spatial; and proceeds may move rapidly across wallets, platforms and states. This article examines three connected problems: attribution of conduct to a legally responsible person, selection and coordination of jurisdiction, and collection of reliable immersive digital evidence. Using doctrinal and comparative analysis, it evaluates the Indian framework comprising the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, alongside emerging international cooperation models. Existing law can address much metaverse-enabled wrongdoing through technology-neutral offences, but important gaps remain where virtual identity, psychological injury, platform control and volatile multimodal evidence do not fit inherited legal assumptions. The article proposes a layered governance model based on functional identity assurance, harm-sensitive offence interpretation, effects-based jurisdiction, rapid preservation, standardized metaverse forensics and accountable platform cooperation. It argues that effective enforcement does not require universal real-name surveillance. It requires proportionate, auditable mechanisms that can connect serious conduct to accountable persons while preserving anonymity, privacy, due process and legitimate experimentation in immersive environments.

Keywords: metaverse; cybercrime; digital identity; avatar; jurisdiction; electronic evidence; virtual assets; India; platform governance.

1 INTRODUCTION

It is important to think of the metaverse not as a website or fully developed piece of tech, but as a socio-technical environment that is continually developing. It encompasses extended reality, persistent virtual worlds, avatars, artificial intelligence, spatial computing, payment systems and in some cases, blockchain-based assets. Users don't just read or post. They seem to share space and to communicate by voice and gestures; they play with objects, with transactions, building up reputations over time. These attributes can enhance social presence and economic engagement, while also introducing new challenges to familiar online risks and vulnerabilities. Inappropriate behaviour that had previously been expressed textually might now manifest as embodied intrusion. When an account is compromised, an avatar, inventory, social

* Research Scholar at Department of Law, Panjab University, Chandigarh, India.

** Research Scholar at NIILM University, Kaithal, Haryana, India.

history and access credentials are transferred in one. A fraud can consist of a fake avatar, an artificial voice, a bad smart contract and a wallet transfer in a matter of minutes¹.

It is not as if every metaverse crime is new. Common types of crime include theft, cheating, impersonation, stalking, intimidation, sexual abuse, obscenity, money laundering and unauthorized access. The challenge is that the metaverse reshapes the reality that those categories are usually based on. The victim is not seeing a real human but rather an avatar (actor) in front of him. The corresponding event could be broadcasted between a headset, a platform server, the cloud provider and the blockchain. The victim and suspect and/or service providers can be in different countries. Evidence is created at a fast pace and can be lost at the end of a session. Some harmful acts result in economic damage; others mainly in invasion of autonomy, dignity or psychological integrity. In this light, Qin, Wang and Hui (2025)² prioritise the idea of identity and unified enforcement in the governance of the metaverse, whereas Efremova and Russkevich (2025)³ focus on anonymity, fuzzy legal status and procedural proof. Mokoena, Papadopoulou and Rodríguez (2023)⁴ also highlight lack of evidence and conflict over territories as key challenges to prosecution.

In this article, three questions are raised. Firstly, how can the law be made to relate the activities of an avatar to a legally responsible person without sacrificing the anonymity that may be desirable? Second, what if the elements of a metaverse crime are spread across different states – which state has the authority to prescribe, investigate and adjudicate? Third, how can multimodal evidence, the meaning of which is dependent on a technical environment, be preserved, authenticated and presented to investigators? The questions are dependent on each other. To be able to perform jurisdiction, the point of attribution is necessary; to prove the point of attribution reliable evidence is necessary; to obtain reliable evidence in a timely manner, a lawful jurisdictional and cooperation mechanism is necessary.

It relies on doctrinal analysis of the Indian criminal laws and cybercrime laws, procedural and evidence laws with a comparative study of the literature and international instruments. It makes two assertions. First, under the current Indian legal framework, there is ample scope for tackling a significant number of offences against persons and property that can be facilitated by the use of the metaverse, including offences relating to unauthorised access or personation, cheating, stalking and intimidation, obscene or sexually explicit content, and laundering of criminal proceeds. Nevertheless, analogical application is problematic in the case of entirely virtual property, where purely psychological injury is the principal injury, where the conduct is materially produced by an AI system, or where the data on the platform is stored outside the country. Second, reforms should target functions, not a premature and comprehensive list of metaverse offenses. Technology-neutral definitions of harm, graded levels of identity assurance, fast data preservation, and standardized data capture and rights-protective cooperation would stand the test of time across virtual environments, rather than a distinct penal code for each.

¹ G. D. Ritterbusch and M. R. Teichmann, "Defining the Metaverse: A Systematic Literature Review," in *IEEE Access*, vol. 11, pp. 12368-12377, 2023, doi: 10.1109/ACCESS.2023.3241809.

² Qin, H. X., Wang, Y., & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanities and Social Sciences Communications*, 12, 194. <https://doi.org/10.1057/s41599-024-04266-w>

³ Efremova M.A., Russkevich E.A. Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development. *Journal of Digital Technologies and Law*. 2025;3(2):187-202. <https://doi.org/10.21202/jdtl.2025.8>.

⁴ Thabo Mokoena, Eleni Papadopoulou, Camila Rodríguez, Cybercrime Prosecution in the Metaverse: Evidentiary and Jurisdictional Challenges, *Legal Studies in Digital Age*: Vol. 2 No. 1 (2023), p. 53.

2 METAVERSE AS A UNIQUE CRIME ENVIRONMENT

There is no universally agreed-upon definition of the metaverse. A useful definition, for purposes of the criminal law, should seek to focus on characteristics that affect opportunities, harm or proof. The metaverse can therefore be defined as a set of digitally mediated environments that can be persistent or recurring, and that provide a sense of spatial presence, synchronous interaction via avatars or agents, creation or possession and exchange of digital objects, and extensive processing of contextual, behavioural or biometric data. The persistence does not imply that all objects must persist forever, and the decentralization is not mandatory. A commercial virtual reality platform can be centrally controlled, while assets and identity credentials can be issued on blockchains and by independent providers⁵.

There are four features which stand out in the environment. First, conduct is endowed with spatial and affective attributes. An intimidating avatar can come closer, accompany, surround or emulate unwelcome contact. Sensory feedback can be provided with haptic devices. According to González-Tapia (2023)⁶, virtual emotions are of legal relevance because experiences experienced through technology can be real fear, humiliation and traumatic experiences. Not touching shouldn't be equated with no damage, especially if it is legally cognizable. Meanwhile, the criminalisation cannot be linked to all unpleasant virtual interactions, but only to deeds of culpability and objectively serious interference.

Second, the value of the identity, and also of property, increases thanks to persistence and portability. An avatar can have a reputation, employment access, creative output and purchased 'wearables' and social relationships. The ability to exchange virtual land, tokens and in-world items for money, and the scarcity of these items by platform design, also add to their value. Cheong (2022)⁷ points out that there are questions in the areas of identity, property, intellectual property, and liability regarding avatars. A pure contract approach – where each asset is a revocable platform licence – may not capture the true reliance and economic loss. On the other hand, making all game objects property for all criminal-law purposes might overcriminalize breaches of the rules within fictional worlds. The parties' reasonable expectations, monetary convertibility, scarcity, and transferability and control should all be analyzed from a legal perspective.

Third, it's a data-intensive environment. Headsets and controllers can capture gaze, voice, facial expression, hand movement, body posture, and room geometry and the proximity to others. This information can be used to recognize users, detect disabilities or emotions, and even recreate actions with a high degree of accuracy. It is both proof and sensitive personal information. Based on this, McStay (2023)⁸ characterizes the metaverse as a surveillant physics, as it is necessary to measure bodies and spaces to render the experience. At the very heart of the resultant paradox is the notion that the most probative record can also be the most intrusive.

Fourthly, the metaverse is a phenomenon of public and private governance. Platform operators write community rules, set safety boundaries, authenticate accounts, moderate behavior and control logs. They can investigate and sanction quicker than states, but with different aims, methods and transparency than criminal justice. Decentralization is not the same as having no control: decentralized autonomous

⁵ Jaber, T. A. (2022). Security Risks of the Metaverse World. *Int. J. Interact. Mob. Technol.*, 16(13), 4-14.

⁶ González-Tapia, M. I. (2023). Virtual emotions and criminal law. *Frontiers in psychology*, 14, 1260425.

⁷ Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, 3(2), 467–494. <https://doi.org/10.1365/s43439-022-00056-9>

⁸ McStay, A. (2023). *Automating empathy: Decoding technologies that gauge intimate life* (p. 304). Oxford University Press.

organizations and smart contracts can distribute control. According to Zwitter and Hazenberg (2021)⁹, technology design itself has a normative power. The state should therefore walk hand in hand with the platforms, rather than delegating the definition of crime and coercive power and the fair procedural rules to the platforms' terms of service.

These features allow a progression of misbehaviors. On one extreme are the standard cybercrimes done in a new way: grabbing credentials, sending out malware and phishing and hacking accounts. Then there are technology enhanced crimes in the middle: deepfake personation, coordinated stalking, extortion with intimate avatar recordings, fraud in virtual asset markets, and virtual wallet layers. On the opposite side of the spectrum are harms that are dependent on the environment, such as simulated sexual contact without consent, manipulation of a child's avatar, or taking something that doesn't exist in reality and therefore has no value. But, as Marshall and Tompsett (2024)¹⁰ rightly warn, the metaverse is not a completely new frontier. But continuity of offence labels should not be confused for changes in scale, intensity and evidentiary structure.

3 DIGITAL IDENTITY, DIGITAL ATTRIBUTION AND CRIMINAL RESPONSIBILITY

3.1 The Layered Identity Problem

In the metaverse, there is multiple layering to identity. A natural person could control multiple avatars, multiple people could share one account, one avatar could be controlled by an organization and an artificial intelligence agent could act with varying degrees of human direction. The presentation layer is using the display name. The layers below include device identifiers, IP records, wallet addresses, payment details, biometric patterns and platform logs, information that provides the necessary credentials for an account. Investigators need to navigate the layers carefully to be able to make attributions.

As a rule, an avatar is not a unique legal entity. The rights, duties, assets and responsibility must be allocated to legal persons, however visually autonomous or conversationally sophisticated the avatar may appear. But there should exist a specialised legitimate interest in the integrity of avatars. Even if the avatar does not have a human-like personality, privacy, reputation, property and personal autonomy can be undermined by unauthorised uptake, misleading reproduction or malicious modification. Mitrushchenkova (2022)¹¹ presents the personal identity in the metaverse as a site of expressive freedom, but also one of vulnerability. The rightful approach is to safeguard the human or organisation portrayed as the avatar and treat the avatar and credentials as evidence and, if appropriate, as proprietary objects.

There are valid reasons for anonymity. It enables social engagement, exploring disabilities, protection for vulnerable people and creative role play. A real name system would produce databases that would be loved by criminals, would allow for profiling, and provide a chilling effect on legitimate use. But full practical non-traceability can cover repeat offenders. A functional or tiered identity assurance is a proportionate model. Low risk social exploration can be pseudonymous. There is a possibility to provide

⁹ Zwitter, A., & Hazenberg, J. (2021). Cyberspace, Blockchain, Governance: How Technology Implies Normative Power and Regulation. In B. Cappiello & G. Carullo (Eds.), *Blockchain, Law and Governance* (pp. 87–97). Springer, Cham. https://doi.org/10.1007/978-3-030-52722-8_6

¹⁰ Marshall, A. M., & Tompsett, B. C. (2024). *The metaverse—Not a new frontier for crime*. *WIREs Forensic Science*, 6(1), e1505. <https://doi.org/10.1002/wfs2.1505>

¹¹ Mitrushchenkova A.N. Personal Identity in the Metaverse: Challenges and Risks. *Kutafin Law Review*. 2022;9(4):793-817. <https://doi.org/10.17803/2313-5395.2022.4.22.793-817>

more robust assurances for higher-risk functions such as large transfers, access to children, professional services, or operating regulated markets. The platform can validate an attribute or the platform could store an encrypted identity link without using a civil name. Disclosure is to take place through the course of a lawful and reviewable process.

3.2 Impersonation, Deepfake and Biometric Mimicry

Metaverse impersonation goes beyond copied usernames. Generative AI can duplicate voice, face, gesture and conversational style. A person trying to defraud may show up in a familiar virtual setting and instruct an employee to move assets to him or her. Biometric information obtained from motion sensors can be played back or used to deduce the identity. While Yang et al. (2023)¹² suggest frameworks for traceable authentication, not all authentication is traceable, as technical systems can be hacked and credentials can be shared, and classifiers of biometric data can be wrong.

There are multiple ways to enter into Indian law. Section 66C of the Information Technology Act, 2000 (IT Act)¹³ covers the criminal use of another person's electronic signature, password or unique identification feature and section 66D of the IT Act covers cheating by personation using a communication device or computer resource. Unauthorized access, copying, introduction of contaminants and related conduct may lead to the imposition of sections 43¹⁴ and 66¹⁵, as long as the aforementioned statutory mental element is fulfilled. The Bharatiya Nyaya Sanhita, 2023 (BNS) includes general provisions of cheating and cheating by personation along with provisions relating to forgery which may be applicable to electronic records. They cover many deepfake-enabled frauds that might take the form of an avatar, and they are technology neutral enough to be applicable.

Gaps nevertheless remain. The specific wording in section 66C would apply best if a defined credential or a unique identification feature is misused. A convincing imitation can be created from publicly available voice and gesture information without the need to steal the credentials. Typically, personation offences will need to involve a degree of cheating, deception, or a similar result, and non-financial identity abuse could be covered by the privacy, defamation and harassment offences. Digital identity interference should be defined in functional terms, namely whether the interference has been intentional, unauthorized; whether it has caused or created a substantial risk of economic loss, reputational injury, sexual exploitation, unlawful access or risk of significant psychological harm. Include defenses where there is no prohibited deception, such as satire, art, research, and authorized simulation.

A person's responsibility for a crime remains the basis of the criminal law. If an AI-controlled avatar causes harm to another user, then the responsibility for the damage needs to be determined based on the connection between the human and the AI. No one should avoid facing the consequences for telling an agent to harass or defraud when that is what the agent was instructed to do, even if the last words were automatic or the last motion was made by the agent. It is the responsibility of a developer or deployer where an offence recognises recklessness, negligence, abetment and conspiracy with elements established. There is, however, no substitute for mens rea beyond simply having a system.

¹² Yang, K., Zhang, Z., Tian, Y. and Ma, J. (2023), A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse. *IEEE Transactions on Information Forensics and Security*, 18: 3817-3832. <https://doi.org/10.1109/TIFS.2023.3288689>

¹³ The Information Technology Act, 2000.

¹⁴ The Information Technology Act, 2000, section 43.

¹⁵ The Information Technology Act, 2000, section 66.

The evidentiary inquiry should clarify the agency chain that leads from the choice of objective through completion of the data, setup of the protective measures, approval of the deployment, keeping of the override power for its own uses and benefit, and the anticipated results. Logs of prompts, model versions and tool calls may be crucial. The risk is hindsight liability – the liability that one can automatically assume just because a complex system caused harm. Multiple actors present challenges when it comes to responsibility for AI as noted by Padovan, Martins and Reed (2023)¹⁶. There is a need to differentiate between whether the fault is committed, using criminal law to punish if it is, and whether the risks are sufficiently serious to warrant civil liability, regulatory measures and action on the platform to remediate.

3.3 Children's Experiences and the Needs of Vulnerable Users

Age deception, grooming, simulated sexual activity and the collection of sensitive data are specific dangers for children. Embodied communication can be more persuasive and thus more immediate in the area of grooming. While age assurance might be accepted for adults, having to take government identity papers from all children may pose another security risk. Use of privacy preserving age estimation or verified age tokens, if possible, including parental tools, child-friendly reporting, and personal boundaries and limits on unnecessary adult-child contact should be encouraged¹⁷.

Transmission or publication within the meaning of the IT Act (including those that could be considered sexually explicit material or material that depicts children) may occur, but not every live embodied misconduct is necessarily a conventionally conceived image or a file. The legal aspect requires focussing on solicitation, grooming, intentional exposure and serious non-consensual simulation and at the same time maintaining the principle of legality. Platform rules may be more stringent than the criminal law as long as they are both known and subject to appeal in enforcement.

4 THE SUBSTANTIVE OFFENCES AND INDIAN LEGAL FRAMEWORK

4.1 Fraud, Unauthorized Access and Virtual Property

Social engineering can be paired with programmable transactions in the metaverse. A user can be tricked into linking a wallet, accepting a malicious smart contract, buying a fake virtual asset, and/or giving too much information to an avatar impersonating a support staff member. Both the IT Act and BNS will offer a practical combination of responses to an unauthorized computer related activity: the IT Act will permit prosecution for unauthorized computer-related activity, and deception and dishonest inducement can be prosecuted as cheating. Anti-money-laundering law applies if the statutory conditions are satisfied in cases where the proceeds are converted or layered using crypto-assets.

Theft of virtual property is more difficult. The traditional approach to theft has traditionally been associated with movable property and the actual taking of the property, but in some cases, a copy of a data source may be made without the original being removed. But for some virtual assets, in practice the control of a token or an account is transferred, and the victim loses the means of using or selling the

¹⁶ Padovan, P.H., Martins, C.M. and Reed, C., 2023. Black is the new orange: how to determine AI liability. *Artificial Intelligence and Law*, 31(1), pp.69-99.

¹⁷ Bagattini, A. (2019). Children's well-being and vulnerability. *Ethics and Social Welfare*, 13(3), 211–215. <https://doi.org/10.1080/17496535.2019.1647973>

asset. Strikwerda (2012)¹⁸ suggests that, besides physicality, the moral and ontological approach to virtual-item theft should not forget the concepts of exclusion and value. The charging, jurisdiction and remedy depend on which of the offenses of non-privileged use for access to computer system, cheating, criminal breach of trust or misappropriation may be applied by prosecutors, if any, on the basis of facts.

A technology neutral, statutory definition of a protected digital asset should acknowledge that a digital asset can be the subject of exclusive control, transfer, valuation or use and that the digital asset is regarded by the parties as having economic or functional value. This does not mean that all game permissions need to be treated as protected digital assets. Courts should take into account the platform agreement, technical architecture, market convertibility and the victim's real loss. Restitution mechanisms should be allowed to return an asset or compensate for an equivalent value, even if criminalization of the confiscation of these sorts of assets is hindered by cross-chain transfers.

4.2 Harassment, Stalking and Immersive Sexual Harm

Persistent following of someone through spaces, threats, disclosure of personal information, the 'recording' of unwanted footage and playing with an avatar's attire, or 'contact with an avatar's sexual parts' may be considered as 'harassing/immersive'. Specific facts may be encompassed by existing offences including stalking, voyeurism, sexual harassment, criminal intimidation, defamation and obscene or sexually explicit publication. But inherited meanings can be based upon physical contact, gender-specific factors, repeated communication, or generation and distribution of content. A single immersive event can occasion grave harm but none of them fit neatly.

There are two extremes in law that should be avoided. Treating any virtual violence as physical violence ignores the statutory requirements and the distinction between simulated and real violence. Treating the event as unreal bypasses embodiment, haptic feedback and psychological harm. A harm and safety concept has been advocated by Chawki, Basu and Choi (2024)¹⁹ which acknowledges the blurred lines between virtual and real world experience. The more effective approach is offence-specific analogy, that is, asking what is the nature of the protected interest that the offence serves: bodily integrity, freedom from fear, protection of reputation, freedom from molestation, sexual autonomy, privacy or other? In each case, the question is whether the metaverse conduct is in some way intended and serious to invade that interest. Legislatures can then fill in tight holes, such as making it a crime to engage in serious, intentional, nonconsensual immersive sex with someone if the perpetrator knows the victim is not consenting, and that the act could reasonably be expected to cause substantial distress in the victim.

Safety by design is required as an accompaniment. Setting personal boundaries to block that immediately removes visibility and audibility, consent prompts to facilitate haptic interaction, default recording notices and accessible reporting can help to prevent or limit harm. These are no excuse for perpetrators or an excuse for the victim to suggest "how could you have been more secure?" Nor should platforms be able to delete evidence in the wake of a report. The interface used for speedy separation should also result in the proportionate preservation of pertinent data.

¹⁸ Strikwerda, Litska (2012). Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. *Ethics and Information Technology* 14 (2):89-97.

¹⁹ Mohamed Chawki & Subhajit Basu & Kyung-Shick Choi, 2024. "Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety," *Laws, MDPI*, vol. 13(3), pages 1-23, May.

4.3 Interconnection of Platforms

Platforms exist in an interstice between the roles of venue, identity provider, evidence custodian, market operator and rule maker. In addition to this, intermediary protection is provided by section 79 of the IT Act²⁰ if it satisfies the due-diligence conditions and if it does not engage in any prohibited action (such as initiating the transmission, choosing the recipient or altering its contents). Services can have a far more active role in the metaverse than the traditional conduits. They can suggest spaces, create avatars, perform asset transfers, handle haptic interaction and remember spatial data. It is important to determine whether a given service serves as an intermediary or is not an intermediary function by function.

Safe-harbour rules should not protect obstruction, the intentional design of criminal markets or failure to abide by lawful preservation orders, but these rules should not preclude innovation or impose blanket monitoring requirements. A code of practice for the metaverse may include guidelines for risk assessment, child-safety defaults, transparent moderation, emergency reporting systems, retention policies, preservation of data and a designated point of contact for law enforcement. Service sizes, functions and risks should be the basis for graduated duties. Compliance can be tested through independent audits and transparency reports, without the need to inspect all interactions.

5 JURISDICTION IN A BORDERLESS BUT NOT PLACELESS ENVIRONMENT

5.1 Multiple Territorial Connections

A metaverse incident can have at least six locations: the victim, the suspect, the access device, the platform company, the processing server and the wallet or asset service. Not all of them are necessarily in a single country. The concept of territorial jurisdiction does however have its uses as people and buildings are physically located. The issue is not the loss of territory, but concurrent jurisdiction.

The typical methods that states use to assert jurisdiction are based on territorial conduct, effects within the state, the nationality of the offender, the nationality of the victim, and protection of essential state interests. In the case of conduct with a computer, computer system or computer network in India, the IT Act has an express provision of extraterritorial application under section 75. The BNS is also extraterritorial in certain situations and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) regulates the place of inquiry and trial of offences and also provides machinery for reciprocal assistance. While these rules may create Indian jurisdiction in numerous instances of cross-border events, it is important to note that legal jurisdiction cannot ensure the means to access a foreign suspect or data.

An effects-based approach is appealing in cases of loss or harm suffered by a victim in India, but the unlimited effects jurisdiction has the risk of global over-reach, as virtually any online conduct is deemed to occur everywhere. A substantial connection test should take into account intentional targeting, foreseeable and significant harm, nationality/habitual residence, critical infrastructure location, and ease of evidence. Multiple states may have a legitimate interest, and prosecutors should coordinate based on factors including: gravity of the case, number and vulnerability of victims, suspect location, comparative evidence collection capabilities, fair-trial rights and risk of double jeopardy.

²⁰ Section 79 of the Information Technology Act provides a “safe harbour” that protects internet platforms from legal liability for content posted by their users.

5.2 Terms of Service Are Not Criminal Jurisdiction

Platform terms often specify a forum and a law to govern contractual disputes. The clauses are inoperative as a basis for a state's criminal jurisdiction. Nor, indeed, can a platform claim to be a legally independent virtual district simply by having users opt for the rules of the community. Private ordering can operate as a means of regulating acceptable behaviour and the ownership of things; public law remains for crime, coercive investigation and rights.

Problems arise in the identification of the responsible recipient for ordering in decentralization. Although there may not be a central headquarters for a protocol, interface operators, validators, wallet operators, developers and/or governance participants or others in their various capacities may exercise differing forms of control over the protocol. The imposition of liability or disclosure obligations should be based on the actual control and legal ability of a project, not on any mere association with a project. Generalizing to open-source developers would put the brakes on innovation and could be problematic for culpability values.

5.3 Cross-Border Cooperation and Speed

Traditional mutual assistance is usually too slow for volatile and mobile data. The difference between disclosure and preservation: A faster order can “preserve” relevant data, and a slower order can determine whether it may be lawfully “disclosed.” This should inform reform. The Budapest Convention's 24/7 Network²¹ provides for urgent assistance and preservation of electronic evidence by its participants and its Second Additional Protocol fosters cooperation with service providers and disclosure of electronic evidence. The UN Convention against Cybercrime adopted by the General Assembly in 2024 establishes a more comprehensive basis for cooperation and electronic evidence, but will only be effective once it is signed, ratified, and given effect.²²

India needs to enhance the existing specialist contact system for availability at all times, and establish a standardized path forward for emergency requests and direct provider contact in line with Indian law. Requests must be specific to the account or session, offence, data categories, time window and necessity. Providers should be cautious to maintain confidentiality and should only disclose accordingly upon Constitutional permission. The dual-criminality requirement can interfere with true innovative harms; states should allow flexibility in how they interpret this based on their underlying conduct and their protected interest, with safeguards against harmful requests or those based on political motives or rights abuses.

Conflicts of law also have an impact on privacy. A disclosure under data protection or constitutional standards of the requesting state may be in contravention of data protection or constitutional standards of the receiving state. Cooperation tools should provide for necessity, proportionality, limitation of purpose, security, deletion and remedies. The users should typically be alerted when there is no longer a need for the seal and providers should be able to contest any order that appears to be unnecessary or too broad.

²¹ Convention on Cybercrime (ETS No. 185), Budapest, 23 November 2001, art. 35.

²² United Nations Convention against Cybercrime, General Assembly resolution 79/243 (24 December 2024), <https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html>.

6 IMMERSIVE DIGITAL EVIDENCE

6.1 What Constitutes a Metaverse Crime Scene

A metaverse crime scene is distributed and layered: account registration and login logs, avatar identity and inventory, voice or text communications, 3D scenes, object and collision logs, headset and controller telemetry, gaze and gesture data, device artefacts, moderation, AI prompts and outputs, smart contracts, blockchain transactions, wallet provider logs, and wallet data. It's not the case that one source captures the event in an exact manner.

A victim's recording will include what was recorded on the victim device and not necessarily what was in the system state. Coordinates can be recorded on a platform log without the cues necessary to interpret them. A blockchain will reliably record a transaction, but it will not make some sort of reflection on whether or not consent was obtained fraudulently. Movement of the device could be connected to a controller, but it would not indicate who was operating the controller at the time of the movement. In this regard, Seo, Seok and Lee (2023) suggest a specific metaverse forensic framework, while AlMutawa, Ikuesan and Said (2024) stress the important issues of mapping forensic tasks and technology²³.

Use of a layered reconstruction model by investigators is recommended. The presentation layer contains information on what the user has heard, seen, or felt. The interaction layer is an application of avatars, communications, and spatial events. Platform logic and moderation actions reside in the application layer. The infrastructure layer contains server, cloud and network data. The transaction layer covers blockchains, wallets and payment rails. The physical layer includes devices, local files and the human environment. Multiple layers of corroboration lower reliance on a single proprietary account.

6.2 Volatility and Preservation

Many immersive events are temporary. Voice might not be maintained, an instance might be closed, and an avatar might change, an AI model might be changed or a smart contract might move the assets automatically. Preservation should start as soon as possible but it should be limited in scope. Platforms should include an in-product evidence hold that is triggered through a serious report, a set period of time in front of and behind a report, and metadata of the participants and integrity of the report. The hold should be backed up and subject to expiry and/or legal extension.

There is nothing that can be substituted for forensic readiness, but there is such a thing as "over-retention". Continuous recording of all users' gaze, rooms and intimate movements would create serious surveillance and security risks. Data minimization and evidence preservation are not mutually exclusive, and can be accomplished via short default retention, event triggered holds, local encryption, separation of identity data and strict access control. Preservation should be auditable and criminal investigators should have lawful permission to add intrusive categories.

²³ Seo, S., Seok, B., & Lee, C. (2023). Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*, 79(9), 9467–9485. <https://doi.org/10.1007/s11227-023-05045-1>; AlMutawa, A., Ikuesan, R. A., & Said, H. (2024). Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model. *Future Internet*, 16(12), 437. <https://doi.org/10.3390/fi16120437>

6.3 Data Pertaining to Authenticity, Integrity and Chain of Custody

Authenticity is the question as to whether it is what its promoter says it is. Integrity: has it changed? Reliability is whether it can be reliably produced. These are overlapping but should not be folded. A correct crypto hash can assure that a file's content hasn't altered since it was collected but doesn't assure that original data was accurately collected. There are no either/or situations with blockchain storage either, as information entered is not validated.

A defensible process should document the collection authority, collector, date and synchronized time source; platform and software version; account, device and session identifier; data schema; how the data was collected; cryptographic hashes; transformations; where the data is stored; who accesses the data where; and each transfer. Proprietary formats should be exported in a native format as well as in an open, documented format. Preserved source data for visualization in court should be repeatable with specifications of assumptions and interpolation clearly stated. In addition, Alruwaili (2021)²⁴ recommends the implementation of distributed chain-of-custody processes; however, technology must complement not supersede the accountable procedure of humans.

Provenance is essential in the case of deepfakes. Experts may have to be called to provide evidence on detection error, compression, artefacts in the model and replay. The party claiming use of the recording is not responsible for proving a negative, but should be responsible for establishing a chain of credibility from source to exhibit. The defence must have adequate access to the underlying data and tools to challenge the prosecution's reconstruction, except in so far as this information is protected by privacy rights orders.

6.4 Evidence and Procedure in India

The Bharatiya Sakshya Adhiniyam, 2023 ("BSA")²⁵ expressly includes electronic and digital records as documentary evidence and lays down conditions for admission of electronic records. It could include records on the platform, wallet transactions, data from devices, and immersive recordings. A critical legal question will typically be whether the electronic record is in compliance with the statutory requirements that specify the way in which an electronic record is to be proven, and the reliability of the system that generated it. A screenshot or exported video can never be considered to be the legally relevant original by investigators.

The BNSS modernizes a number of aspects of the procedure, such as the acceptance of electronic communication and audio-video in criminal process. Search, seizure, forensic examination and reciprocal assistance powers can be used to aid investigation of metaverse cases. However, a traditional mindset about devices and seizures will not suffice if a key record is stored in the cloud somewhere other than your jurisdiction or on an out-of-control distributed ledger. Operational protocols should clearly define the process used to request emergency hold, capture virtual scene live, image off a headset, get a platform schema, trace a wallet, and document software dependencies.

Specialised forensic labs and trained examiners are required. Teams might need specialists in the area of virtual reality, network forensics, blockchain analysis, AI provenance, trauma-informed interviewing,

²⁴ Alruwaili, F. F. (2021). CustodyBlock: A Distributed Chain of Custody Evidence Framework. *Information*, 12(2), 88. <https://doi.org/10.3390/info12020088>

²⁵ Sections 57 and 61 classify electronic and digital records as valid documents and primary/admissible evidence on par with physical records.

and comparative law. The problem of interpretative error is also prevented by a multi-disciplinary approach. An avatar animation could be one that the platform generates automatically—or one the user selects; the forensician can describe the animation system, and investigators can evaluate communications around that intent.

6.5 Privacy, Privilege and Due Process

Metaverse evidence can reveal bystanders, private residences, health issues, and intimate behaviour and relationships. Religious items or medication could be found during a room scan taken as part of a play boundary. The gaze data can reveal interests or impairment. A broad warrant for an entire history of an account is thus disproportionate. Orders must be subject to time limits, the number of participants, data type and alleged offence with special justification for biometric and spatial-home data.

Privileged communications and irrelevant third parties should be protected in filtering. Investigators should capture results of automated analytics and report on material error rates. Any indication of suspicious gesture(s), match of voice(s) or reconstruction of a scene by AI must be treated as an investigative lead unless independently validated. The accused should be able to adequately challenge the model, the data and any inferences made²⁶. There are also issues of equality as the biometric and speech systems could function differently between populations.

Victims need control and support. Trauma-informed collection should involve as little re-exposure to recordings as possible, provide clear options regarding sensitive content, and clarify disclosure in court proceedings. At the same time, the right to safety cannot be deemed in and of itself a proof of guilt, because of the right to due process. Criminal adjudication is based on separate evidence that is tested substantially in accord with law.

7 A COORDINATED REGULATORY MODEL

The analysis suggests a multi-layered approach in the form of statutes instead of a single metaverse statute. It consists of five layers, the first being substantive criminal law. Offences already defined as technology neutral should be applied as appropriate if the elements of these offences really apply. Legislatures should only include an exception for specific problems or narrow exceptions that have been proven, specifically, and especially, digital-identity interference and protected digital assets and intentional non-consensual immersive sexual conduct. Drafting should be directed towards control, human influence, deception, consent, harm and culpability, and not at particular brands or equipment.

The second layer is procedural readiness. The law should differentiate between urgent preservation and disclosure, provide for limited and targeted cross-border requests, and set up expedited judicial review. A ‘standard metaverse evidence-preservation notice’ stating identifiers, relevant time periods, categories and retention time period could be implemented in India. There should be a designated 24/7 contact point for coordination with platforms and foreign counterparts, and have an open log of requests and results.

²⁶ Gulati, P., Pal, K. (2024). The Notion of Privacy Rights in the Metaverse: Examining Legal Hemispheres in India’s Digital Era. In: Kautish, S., Rocha, Á. (eds) *Metaverse Driven Intelligent Information Systems*. Information Systems Engineering and Management, vol 20. Springer, Cham. https://doi.org/10.1007/978-3-031-72418-3_10

Forensic standardization is the third layer. Minimum acquisition and chain of custody fields, for immersive evidence, should be defined in a national protocol, including time synchronization, coordinate systems, software versions, rendering parameters, AI involvement and cryptographic integrity. Export formats should be interoperable and include data dictionaries. VR scene reconstruction and blockchain analysis should also be assessed and accredited, in addition to proficiency testing. The protocol should be created in consultation with forensic institutes, courts, law enforcement and defence lawyers, platforms and civil-society experts.

The platform governance layer is the fourth layer. Services should be designed to be safe, have multiple tiers of identity assurance, evidence holds, accessible reporting and child protection, along with a lawful-request interface. There is a link between working practices and risk. It isn't fair to impose compliance obligations on a small creative world that would apply to a big financial marketplace or kids' space. Safe harbour should remain for good-faith intermediaries, but responsibilities for transparency and preservation should come into play for functions where a platform has control over risk and evidence.

The fifth layer is rights oversight. Intrusive identification and access to data should be supervised by independent authorities and courts. There should be an aggregate transparency report that includes the number of preservation and production requirements, number of emergency requests, rejection rates and transfers across national borders. There should always be remedies for wrongful disclosure, retention of identity over and above the need and retention beyond lawful need. To mitigate the false choice between accountability and anonymity, available privacy-enhancing technologies include selective-disclosure credentials, encrypted identity escrow and zero-knowledge age proofs.

In the international context, elements of harmonisation should focus on the procedure and on the minimum offence concepts and not on uniform cultural regulation of all virtual behaviour. Agreements can be made regarding expedited preservation, points of contact, authenticity documentation, asset freezing, and asset safeguards despite any differences in substantive laws. The Budapest system provides lessons for operation and the UN Convention against Cybercrime provides a potentially broader ground for cooperation. There should be a review of the implementation of these in light of human rights, since the scope of cybercrime powers could be used for surveillance or suppression of expression.

Lastly, regulation should be an ongoing process. Mandatory incident reporting and anonymised empirical studies can tell us what harms do, and how harms are not addressed through platform controls, or by prosecution. Speculative offences can be prevented from becoming permanent via sunset clauses or periodic review. Regulatory sandboxes can be used to trial age-assurance mechanisms, evidence export and privacy-preserving identity systems — but only under regulatory guidance. The objective is to be adaptable at all institutions and not to predict all future virtual worlds.

8 CONCLUSION

Embodiment, persistent identity, virtual economies and pervasive sensing exacerbate vulnerabilities already seen in digital criminal justice systems in general in the metaverse. The key legal issues are who is responsible, jurisdiction, and obtaining adequate evidence. Avatars can be a useful tool for helping to bring people to life, but they will not create a new legal person. A virtual asset need not be regarded as property in order to be protected. A violation, even if it is not literally translated as physical contact, can

be very serious and cause significant damage. The differences can help keep law principled amidst technological change.

The IT Act, BNS, BNSS and BSA offer a good base for India. They can respond to unauthorized access, identity theft, personation, cheating, stalking, intimidation or illegal content/digital records. However, enforcement efforts will continue to be uneven, with the absence of clarity in the law and practice on digital identity interference, virtual-asset control, immersive sexual harm, platform preservation and cross-border access. Reforms that are functional and procedural – graded identity assurance, a significant connection regime, prompt preservation that is subject to review, standardized multimodal forensics, and duties on the platform based on risk – are the most useful.

Accountability is possible without the omnipresence of identification. The values of lawful pseudonymity, experimentation, and intimate association deserve to be protected, and the metaverse can enable these values. A legitimate structure will link serious wrongdoing with responsible individuals using a proportionate process, rather than through the blanket of surveillance. Technologically neutral criminal law, focused cooperation of specialists, forensic precision and protection of rights can help shield victims, while respecting the rule of law and due process, as 3D environments become a commonplace part of social and economic interaction.

* * *