Beyond Territorial Sovereignty:

Reconstructing Legal Integrity in the Metaverse

By Tejpratap Singh

VOLUME I | ISSUE I | ARTICLE VI

APRIL 2026

The Legalis IP Quarterly

ABSTRACT

The arrival of the virtual reality-based metaverse has raised complex legal issues across countries worldwide. These legal systems are ever-evolving; however, in the context of the metaverse, which is itself transitional and immaterial, keeping up with legal developments has become a complex challenge.

The current global technological laws have territorial jurisdiction. Only a few jurisdictions, such as the European Union, the United States, China, Singapore, and the United Arab Emirates, have developed relatively advanced legal frameworks for digital assets. Most other countries have not made comparable progress in regulating the metaverse, largely because of its borderless nature, which transcends territorial laws and conventional jurisdictional boundaries. It thus becomes incredibly complicated to impose municipal laws on the use of the metaverse. These raise genuine questions, such as who should be held accountable for arising liabilities, who will have jurisdiction to preside over any violations of intellectual property (IP) in the metaverse, and which laws would specifically apply.

The scope of this research will be on the jurisdictional friction between sovereign states and Decentralised Autonomous Organisations (DAOs). It will also investigate the civil liabilities that have arisen from disputes over virtual property and the regulatory gaps that exist in the protection of the user's "Biometric Sovereignty" within the existing framework of international data privacy laws.

The central argument is that the current "Westphalian" architecture of territorial sovereignty is incapable of transitioning to the decentralised model of the metaverse. This research is to find out and prevent global 'regulatory race to the bottom', So that the international community can adopt a system

of metaverse-specific laws or "Lex Metaversi", a self-implied, code based on legal framework which uses smart laws (laws embedded through coding in the system so that it can be self-imposed) to enforce IPR and commercial agreements automatically, therefore replacing reactive litigation with proactive, algorithmic integrity.

Keywords: *Metaverse; jurisdiction; territorial sovereignty; Westphalian sovereignty; decentralised autonomous organisations (DAOs); virtual property; civil liability; intellectual property rights; digital assets; biometric sovereignty; data privacy; international data protection law; cross-border regulation; regulatory gaps; lex metaversi; smart contracts; code-based governance; algorithmic enforcement.*

I. INTRODUCTION

The rapid transition of the global digital order from the two-dimensional, screen-mediated interfaces of Web 2.0 to the three-dimensional, immersive environments commonly described as the metaverse marks a fundamental shift in social, economic, and legal interactions.[1] As this technological transformation accelerates, the idea of legal integrity, understood as the coherence, ethical alignment, and effectiveness of regulatory frameworks across both physical and virtual domains, becomes central to contemporary legal thought.[2] The metaverse is not merely a collection of gaming platforms; rather, it is a collaborative virtual space shaped by the convergence of enhanced physical reality and persistent digital environments, thereby challenging traditional legal concepts such as territorial sovereignty, personal identity, and property rights.[3] The current legal landscape remains marked by significant regulatory gaps and fragmented ethical standards, as existing digital and technological laws often provide vague or inadequate definitions of foundational concepts. Such shortcomings risk generating legal uncertainty, ethical dilemmas, and a broader erosion of public trust in digital institutions. For the metaverse to

[1] Oleksandr Baranov et al., Digital Transformations of Society: Problems of Law, (2026) https://www.researchgate.net/publication/379237287 [https://doi.org/10.31435/rsglobal/057].
[2] Oleh Semenenko et al., Forecasts of Transformation in Legal Regulation of Artificial Intelligence for Cybersecurity in Ukraine's Defence Sector, (2025) https://www.researchgate.net/publication/398050452 [https://doi.org/10.18226/25253824.v9.n14.02].
[3] Mariia Viktorivna Dubniak, Digital Transformation from Informatization to Artificial Intelligence in Administrative Services in Ukraine, (2024) https://www.researchgate.net/publication/387940489 [https://doi.org/10.69635/978-1-0690482-1-9-ch15].

achieve legal integrity at the global level, a doctrinal transformation is required, one that moves beyond isolated domestic approaches towards a transborder standard model capable of harmonising legal and technical norms across decentralised ecosystems.

In this context, the present study adopts a doctrinal and comparative methodology to analyse the emerging legal challenges posed by the metaverse. It critically examines existing legal regimes, particularly the Information Technology Act, 2000 and the European Union's General Data Protection Regulation, to identify jurisdictional gaps in decentralised digital spaces.[4] It also employs a comparative approach to evaluate how the United States, the European Union, and India regulate virtual property and biometric information within their respective legal systems. By integrating primary legal materials, such as statutes, regulations, and relevant legal principles, with secondary academic and analytical sources, this paper develops an analytical framework for governance in the metaverse. Against this backdrop, the study explores the multifaceted legal issues surrounding metaverse regulation, with particular emphasis on intellectual property, jurisdictional conflict of laws, and the pressing need for a coherent global governance framework.

II. EVOLUTION OF DIGITAL PERSONA AND IDENTITY

Human identity has increasingly extended into the online sphere through the notion of the "digital persona", which functions as a necessary representation of the self in a networked society. Alongside it, a related layer of identity has emerged, sometimes described as the "digital unconscious".[5] At present, however, technological systems largely determine how digital identity is constructed, often relying on data mining and profiling to reduce fluid, complex human individuality into rigid, generalised categories. In the absence of coherent legal and ethical frameworks, society, institutions, and experts remain at a fragile, insufficiently developed stage in understanding the implications of these digital selves.[6]

[4] H. Krasnostup, New Media Formation and Prospects of Legal Regulation, (2012) https://www.researchgate.net/publication/367507277 [https://doi.org/10.37750/2616-6798.2012.2(5).271844].
[5] O. Baranov, Civilization Mission of Digital Transformations, (2023) https://www.researchgate.net/publication/373970035 [https:doi.org/10.37750/2616-6798.2023.3(46).287067].
[6] Oleksii Kostenko, Artificial Intelligence (AI) and the Metaverse: Legal Aspects, (2022) https://www.researchgate.net/publication/363777021 [https://doi.org/10.32782/2524-0374/2022-8/66] (last visited Apr. 11, 2026).

The development and operation of the digital persona are shaped by four principal forms of agency: personal agents, namely individuals who often lack technical knowledge and awareness; technological agents, including software systems that frequently depend on stereotyped profiling; institutional and legal agents, whose regulatory frameworks remain inadequate to prevent misuse; and communal agents, such as peers and commercial actors, who may interact with or exploit digital data in ethically problematic ways.[7] Addressing these vulnerabilities requires a comprehensive and interdisciplinary framework rather than isolated technological solutions. Such a framework should integrate insights from sociology, systems engineering, data representation, and network science to enable individuals to manage their digital personae in a secure, ethical, and informed manner.[8]

III. PROBLEM OF IDENTITY VERIFICATION IN DECENTRALISED SPACES

While digitalisation has made contemporary life more efficient, it has also rendered individual privacy increasingly vulnerable, as digital identities are often stored in centralised systems that give users only limited control over their data.[9] Decentralised identity offers an important alternative by enabling individuals to control their credentials across distributed networks and reducing reliance on centralised points of failure.[10] Its practical adoption, however, faces a serious obstacle. If decentralised identity systems require users to manage complex cryptographic keys or navigate unintuitive interfaces, many are likely to abandon them in favour of familiar but less secure centralised platforms, thereby undermining the very purpose of decentralised identity.

A viable decentralised identity framework must therefore prioritise usability. The management of digital credentials should be as simple and accessible as using an online banking application. Achieving this objective requires international cooperation to develop widely accepted verification protocols, together

[7] Griselda Acosta, Eric Smith & Vladik Kreinovich, Analytical Techniques for Gauging Accuracy of Expert Knowledge: A Simple System-Based Explanation of the Dunning-Kruger Effect, (2020) https://www.researchgate.net/publication/341183632 [https://doi.org/10.1007/978-3-030-46413-4_6].
[8] O. Baranov, Social and Digital Transformation: A Source of Legal Problems, (2021) https://www.researchgate.net/publication/356238670 [https://doi.org/10.37750/2616-6798.2021.3(38).243807].
[9] D. de Kerckhove & C. Miranda, What is a digital persona? (2014) https://addi.ehu.es/bitstream/handle/10810/71850/Texto_De_Kerckhove_Miranda.pdf?sequence=1&isAllowed=y [https://doi.org/10.1386/tear.11.3.277_1].
[10] Saurav Bhattacharya, *The Paradox of Progress: Can Decentralized Identity Fix the Privacy Crisis?*, Forbes Nonprofit Council (Nov. 6, 2024 at 07:30 EST), https://www.forbes.com/councils/forbesnonprofitcouncil/2024/11/06/the-paradox-of-progress-can-decentralized-identity-fix-the-privacy-crisis/ [https://perma.cc/CR8L-DKX9] (last visited Apr. 11, 2026).

with balanced regulatory frameworks that protect users without impeding innovation. For businesses, the transition to user-controlled identity systems may demand significant investment in technology and training, but it also offers substantial long-term benefits. By reducing the need to store sensitive personal data, firms can lower the risk of major data breaches, ease compliance burdens under regimes such as the General Data Protection Regulation, and foster greater transparency and trust in their relationships with users.[11]

IV. INTELLECTUAL PROPERTY LAW CHALLENGES IN METAVERSE

As the digital persona extends into immersive, decentralised environments commonly described as the metaverse, the convergence of virtual and augmented reality with blockchain raises significant intellectual property challenges. One major concern relates to the protection of valuable virtual goods, including digital wearables, virtual real estate, and other digital assets, which are increasingly vulnerable to unauthorised reproductions of well-known brands. Nike's action against StockX over NFTs linked to Nike-branded sneakers illustrates how digital replication can dilute brand value and mislead consumers. In response, major companies have begun registering trademarks for virtual goods and services to secure their presence in digital environments.

The metaverse also depends heavily on user-generated content, which complicates ownership and enforcement. Platforms such as Roblox often require users to grant broad licences over their creations, raising concerns about the fair allocation of rights and the potential exploitation of creators.[12] At the same time, users may reproduce protected works, create virtual replicas of famous structures, or design avatars and accessories incorporating trademarked elements. Platform moderation systems, which often rely on automated detection, are poorly equipped to assess legal distinctions such as fair use, parody, or transformative use. As a result, unlawful uses may persist, while lawful expression may also be incorrectly restricted.

These difficulties are compounded by the decentralised structure of virtual environments, which weakens traditional territorially grounded enforcement mechanisms.[13] Infringers may operate across

[11] *Id.*
[12] *Terms of Use,* Roblox Corp., https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use [https://perma.cc/U6QL-QJRA] (last visited Apr. 11, 2026).
[13] Eur. Union Intell. Prop. Off., Impact of the Metaverse on Infringement and Enforcement of Intellectual Property (2024) https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Impact_of_t

jurisdictions through pseudonymous accounts, making it difficult for rights holders to identify responsible actors or pursue effective remedies.[14] Although NFTs and smart contracts offer certain technological advantages, including verifiable ownership records and automated royalty payments, their practical use remains limited by regulatory uncertainty, uneven adoption, and fragmented legal frameworks.[15] A more coherent and internationally coordinated legal response is therefore necessary if creativity and commerce are to coexist sustainably in the metaverse.

V. ENFORCEMENT OF IP RIGHTS IN A BORDERLESS DIGITAL SPACE

A new frontier of intellectual property (IP) enforcement in this metaverse world is largely characterised by the decentralised and borderless nature of virtual worlds. IP enforcement relies traditionally on jurisdictional boundaries. All the traditional mechanisms of enforcement become difficult to sustain in the metaverse, where fake digital products, unauthorised replicas, and IP violations may circulate across topographies and platforms with little to no constraint.

A key difficulty lies in the very structure of digital spaces. The obscurity of such blockchain-based platforms makes enforcement much harder. Frequently, IP possessors cannot identify the infringers or bring legal action against individuals who work under aliases or across multiple platforms. The absence of legal harmonisation compounds the problem. IP laws vary significantly across jurisdictions, and the lack of harmonisation exacerbates enforcement challenges in the metaverse, as legal systems have not uniformly adapted to virtual goods and related digital assets. While some jurisdictions recognise digital trademarks and other rights for virtual products, others have yet to develop a coherent framework to address these emerging issues.[16]

VI. INTERNATIONAL AND NATIONAL IP LAWS IN THE METAVERSE

he_metaverse_on_IP_infringement_and_enforcement/Impact_of_the_metaverse_on_IP_infringement_and_enforcement_FullR_en.pdf [https://perma.cc/5VS9-QRU4] (last visited Apr. 11, 2026).

[14] Eleonoea Rosati, *From Web 2 to Web 3: Harnessing Blockchain Technology for* IP, EUR. UNION INTELL. PROP. OFF., (Jan. 01, 2024), https://www.euipo.europa.eu/en/news/from-web-2-to-web-3-harnessing-blockchain-technology-for-ip [https://perma.cc/YX3H-KWWB].

[15] Lawrence R. Helfer, *Human Rights and Intellectual Property: Conflict or Coexistence?,* 5 MINN. INTELL. PROP. REV. 47, 47-61 (2003). https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1399&context=mjlst& [https://doi.org/10.24926/15529541.3758].

[16] Helfer, *supra* note 15.

It is essential to understand how both municipal and international IP rights are protected through multilateral instruments such as the Berne Convention for the Protection of Literary and Artistic Works and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).[17] These instruments establish the basic framework for copyright, trademark, and patent protection. Their application to the metaverse, however, raises difficult questions about cross-border disputes, legal harmonisation, and the development of norms governing virtual assets and digital transactions.

Domestic IP laws vary considerably in their scope, duration, and enforcement mechanisms. In the metaverse, where users and creators frequently operate across multiple jurisdictions, this diversity creates legal uncertainty; thus, it is imperative that global norms, rather than domestic laws, govern virtual assets and transactions. In the United States, the Digital Millennium Copyright Act provides an important framework for addressing digital copyright issues, including those arising from user-generated content. In the Metaverse, where users and generators frequently gauge multiple authorities, the interplay between public IP laws and the need for harmonisation poses challenges. National laws may need to adapt to accommodate virtual means, user-generated content, and cross-platform deals.[18] In the United States, the Digital Millennium Copyright Act provides an important framework for addressing digital copyright issues, including those arising from user-generated content. Comparable legislation exists in other jurisdictions, but its operation and limitations in immersive virtual environments require closer examination.[19]

VII. DOCTRINAL ASPECT OF THE METAVERSE

The metaverse is examined here through a doctrinal method grounded primarily in library-based legal research. That method involves the close and systematic analysis of primary legal materials, including statutes, regulations, policies, judicial decisions, and international instruments, alongside secondary sources such as academic commentary and scholarly treatises.

[17] Andy Ramos, *The Metaverse, NFTs and IP Rights: To Regulate or Not to Regulate?*, WIPO Mag., June 19, 2022, https://www.wipo.int/en/web/wipo-magazine/articles/the-metaverse-nfts-and-ip-rights-to-regulate-or-not-to-regulate-42603 [https://perma.cc/UAG3-CTSW].
[18] Neha Ahuja, *Commercial Creations: The Role of End User License Agreements in Controlling the Exploitation of User Generated Content*, 16 J. Marshall Rev. Intell. Prop. L. 383 (2017) https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1416&context=ripl [https://perma.cc/9L9G-XUFW].
[19] Sagnik Roy Choudhury, *Trademark Law and E-Commerce: A Review of Legal Challenges and Consumer Protection*, 12 TIJER 4 (2016), https://tijer.org/tijer/papers/TIJER2504160.pdf [https://perma.cc/5T6V-W2YK].

In the context of the metaverse, doctrinal analysis does more than describe existing law. It also tests the capacity of established legal doctrines to respond to immersive and technologically mediated environments.[20] This approach has been applied across several important areas of metaverse law, particularly IP, virtual identity, and platform governance. In copyright law, it is used to assess whether digital assets and user-created avatars may qualify as protectable works, and to examine how platform terms allocate ownership and liability.[21] In trademark law, doctrinal and comparative analysis has exposed the limits of concepts such as "trademark use" and "likelihood of confusion" when applied to platform-based infringement, decentralised advertising practices, and third-party digital sellers.

A similar method has been used in patent law to evaluate whether metaverse-related software and virtual technologies satisfy conventional requirements of novelty and inventive step under existing patent regimes. In criminal law, doctrinal analysis has drawn attention to the inadequacy of traditional offences, particularly where legal definitions continue to depend upon physical contact or bodily harm. Such limitations have prompted some scholars to consider alternative frameworks for addressing harmful conduct committed through digital avatars and virtual environments. The same method has also been used to assess national legal preparedness for the metaverse. For example, textual analysis of Malaysian law has been employed to evaluate the adequacy of existing rules on communications, data protection, contracts, misinformation, virtual harassment, and smart contracts.[22]

VIII. SHOULD THE METAVERSE BE GOVERNED AS A DISTINCT LEGAL JURISDICTION?

The broader internet was eventually brought within the reach of domestic legal systems, but the metaverse presents a stronger case for distinct regulatory treatment because of its immersive, three-dimensional, and quasi-spatial character. These are the primary arguments for treating the metaverse as its own governance, along with the proposed structures and challenges involved.[23]

---

[20] Divya Gopalkrishnan, *Sexual Exploitation of Avatars in the Metaverse: An Intellectual Property Perspective*, 15 Int'l J. Sci. Res. 2 (2026), https://www.ijsr.net/archive/v15i2/SR26210215008.pdf [https://doi.org/10.21275/SR26210215008].
[21] Hafidz Hakimi Haron & Nadiah Arsat, *Zuckerberg's Metaverse and the Unready Malaysian Laws: Quo Vadis?*, Proceedings of the International Conference on Law and Digitalization (ICLD 2022) 123, 123-135 (2022) https://www.atlantis-press.com/proceedings/icld-22/125979423 [https://doi.org/10.2991/978-2-494069-59-6_12].
[22] Ananya Khandare, *The Metaverse: Intellectual Property Challenges in a Virtual World*, (Mar 6, 2025 at 11:43 IST) http://www.globalpatentfiling.com/blog/The-Metaverse-Intellectual-Property-Challenges-in-a-Virtual-World [https://perma.cc/UC9S-R4ES] (last visited Apr. 11, 2026).
[23] Jesse Valente, *Governing the Metaverse*, 9 U.C. Intell. Prop. & Comp. L.J. 2, (2024) [scholarship.law.uc.edu/cgi/viewcontent.cgi?article=1056&context=ipclj] [https://doi.org/10.2139/ssrn.4875434].

Existing legal frameworks remain deeply rooted in physical territory and sovereign jurisdiction. When applied to decentralised and borderless virtual environments, they encounter structural limits, procedural gaps, and interpretive uncertainty. Attempting to fit the metaverse entirely within these inherited frameworks may produce regulatory inconsistency, jurisdictional conflict, and unnecessary constraints on innovation.[24]

A separate governance framework is often defended on grounds of uniformity, efficiency, and institutional suitability. National laws differ significantly in scope and operation, which makes the application of territorially bounded rules to immediate and global virtual interactions increasingly impracticable. A more tailored metaverse framework could provide greater predictability and coherence. It could also support specialised legal mechanisms designed for virtual assets, digital property disputes, avatar-based rights, and other questions that do not fit comfortably within conventional legal categories.

IX. HOW A METAVERSE JURISDICTION COULD FUNCTION GOVERNING THIS DISTINCT SPACE REQUIRES INNOVATIVE, DIGITALLY NATIVE MECHANISMS

A proposed model of metaverse governance includes several interrelated elements. Dispute resolution could be conducted through virtual courts and arbitration panels operating entirely within the digital domain. Enforcement, in turn, could rely on smart contracts and blockchain systems to automate compliance and preserve tamper-evident evidentiary records, thereby reducing dependence on traditional physical authorities.

To balance user autonomy with safety, a mongrel governance model is proposed. Under such a model, centralised oversight would ensure coherence, accountability, and institutional coordination, while decentralised, blockchain-enabled rights would protect users in a manner analogous to a digital "bill of rights".[25] Effective digital identity verification would form an equally important part of this framework. Robust verification norms, potentially supported by blockchain-based or comparable identifiers, would be necessary to reduce the anonymity that shields unlawful conduct while still preserving user privacy.

---

[24] Jean-Thomas Arrighi de Casanova, *The Making of the 'Mongrel Nation' – Migration and Territorial Rescaling in Scotland, 1800–1997*, Conference Paper, IMISCOE Annual Conference, Madrid, Spain (Jan. 2016), https://www.researchgate.net/publication/320106960 (last visited Apr. 11, 2026).

[25] David Chalmers, *What Should Be Considered a Crime in the Metaverse?*, WIRED (Jan. 28, 2022, at 09:00 ET), https://www.wired.com/story/crime-metaverse-virtual-reality/ (last visited Apr. 11, 2026).

Metaverse governance, however, cannot exist in complete isolation from the physical world. Conduct within virtual environments, including financial investments, disputes over digital property, and psychological harm arising from virtual misconduct, may have direct and serious real-world consequences.[26]

Traditional governments are therefore unlikely to remain passive where the interests of their citizens are materially affected. Large-scale fraud or substantial economic loss, for example, would almost certainly trigger state intervention. These interconnections point to the need for structured inter-jurisdictional cooperation rather than absolute legal separation. Legal scholars and international organisations have accordingly proposed a framework for relations between virtual and physical legal orders. Such a framework could involve transnational bodies, including the World Intellectual Property Organization, developing model guidelines, bilateral arrangements, and harmonised norms capable of addressing disputes that move across both realms.

[27]

X. THE JURISPRUDENTIAL IMPACT OF HERMES V. ROTHSCHILD

The *Hermès v. Rothschild*, or "MetaBirkins", dispute occupies an important place at the intersection of traditional trademark law and emerging digital markets. The dispute arose when digital artist Mason Rothschild created and sold NFTs associated with images of the Hermès Birkin bag, prompting Hermès to bring claims for trademark infringement, dilution, and cybersquatting. In resolving the matter, the court applied the *Rogers v. Grimaldi* framework in order to balance the avoidance of consumer confusion against the artist's First Amendment interests. The jury ultimately found in favour of Hermès, concluding that Rothschild's use of the Birkin mark was explicitly misleading and awarding damages.

[26] Will Oremus, *Kids Are Flocking to Facebook's 'Metaverse.' Experts Worry Predators Will Follow*, WASH. POST (Feb. 7, 2022), https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/ (on file with Legalis IP Quarterly); *see also* Anna Maria Collard, *Crime in the Metaverse Is Very Real. But How Do We Police a World with No Borders or Bodies?*, WORLD ECON. FORUM (Aug. 18, 2022), https://www.weforum.org/agenda/2022/08/crime-punishment-metaverse/ (last visited Apr. 11, 2026).

[27] Thayssa Bohadana Martins, *Beyond the Bag: MetaBirkins, Hermès, and the Legal Frontier of NFTs in Trademark Law*, 10 BOLOGNA L. REV. 1 (2023), https://bolognalawreview.unibo.it/article/download/20653/20156/98548 [https://doi.org/10.6092/issn.2531-6133/20653].

The verdict suggested that the NFTs functioned less as protected artistic expression and more as commercial products.[28]

The jurisprudential impact of this verdict is profound, serving as a critical litmus test for how courts will regulate brand identity and creative expression in the metaverse. It provides brand owners with the confidence that their intellectual property rights remain enforceable in virtual environments, establishing that major brands and individual digital creators can be considered direct competitors in the digital space. Likewise, the ruling emphasises that while digital art may retain suggestive rudiments, its commercialisation and branding can still infringe upon established trademarks if it exploits a brand's precisely curated exclusivity and consumer goodwill. Accordingly, this corner case is acting as a catalyst for companies worldwide to proactively acclimatise their legal strategies and register their trademarks specifically for virtual goods.[29]

Artists should take note that it is not the creation of art that is problematic, but rather the manner in which it is branded and packaged to consumers that can infringe on intellectual property rights. It is important to remember, however, that the 'MetaBirkins' case was a US federal jury trial and did not establish any mandatory legal precedent.

In addition, the US Supreme Court is set to hear oral arguments in March in *Jack Daniel's v. VIP Products*, where it will determine whether the humorous use of another's trademark as one's own commercial product is subject to the likelihood-of-confusion analysis used in the 'MetaBirkins' case, or protected under the First Amendment.[30]

XI. WHO WILL BE HELD LIABLE?

Responsibility for intellectual property violations in the metaverse primarily falls on direct infringers and online service providers (OSPs). Direct infringers include individuals or entities that produce, mint, or vend unauthorised digital means, as demonstrated by the case of digital artist Mason Rothschild, who

[28] Hari Priya K., *Adapting to Technological Inventions in Metaverse: Challenges in Indian Patent Law Through Case Law Analysis*, 6 Int'l J. Legal Sci. & Innovation 6 (2024), https://ijlsi.com/wp-content/uploads/Adapting-to-Technological-Inventions-in-Metaverse.pdf [https://doij.org/10.10000/IJLSI.112306].

[29] Danielle Garno & Krithika Rajkumar, *Hermès Win in MetaBirkin Trial: Implications for Fashion Industry*, Global Legal Post (Feb 13, 2023), http://www.globallegalpost.com/news/hermes-win-in-metabirkin-trial-implications-for-fashion-industry-1225165154 [https://perma.cc/S4JG-T2FV]

[30] Bohadana Martins, *supra* note 27.

was held liable for trademark infringement, dilution, and cybersquatting for creating and dealing in unauthorised "MetaBirkins" NFTs. Attribution at the individual level, however, is often complicated by the pseudonymous and decentralised character of blockchain-based environments. Infringers may operate under aliases across multiple platforms, making identification and enforcement considerably more difficult for rights holders. These practical difficulties have prompted increasing attention to the role of platforms that host, facilitate, or distribute infringing content. As a result, rights holders have argued with greater force that online service providers should bear a share of legal responsibility where direct enforcement against individual actors proves ineffective. The scope of such platform liability, however, differs significantly across jurisdictions.[31] The US frequently relies on the Digital Millennium Copyright Act (DMCA) notice-and-takedown framework. The European Union, on the other hand, has moved in a more interventionist direction by imposing affirmative duties on platforms to address violations proactively. Other jurisdictions, including Australia, have adopted more specific statutory approaches to intermediary or secondary liability, although the extent to which such models can be adapted to metaverse disputes remains contested.[32]

XII. WHERE WILL DISPUTES BE RESOLVED?

The borderless, decentralised nature of the metaverse disrupts traditional, terrain-grounded legal authorities. Presently, physical-world public courts retain jurisdiction over metaverse controversies because the fiscal and reputational impacts of virtual violations eventually carry over into the real world. For example, the United States Federal Courts assumed jurisdiction over the trademark controversies in *Hermès v. Rothschild* and *Nike v. StockX*. At the same time, Spanish marketable courts oversaw the *Vegap v. Mango* dispute regarding the unauthorised digitisation of physical oils. The application of domestic law to a global and technologically diffuse environment, however, often produces fragmented enforcement and considerable interpretive uncertainty.[33] To address these inefficiencies, legal scholars advocate treating the metaverse as a distinct legal regime. This approach proposes the creation of digitally native dispute-resolution mechanisms, similar to virtual courts operating entirely in the digital

[31] Maeve Hyer, *Physical Sports Needing Virtual Boundaries? An Analysis of Intellectual Property Issues Arising from Sport NFTs*, Intellectual Property Issues Arising from Sport NFTs, 30 Jeffrey S. Moorad Sports L.J. 91 91-16 (2023) digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1422&context=mslj.
[32] Hari Priya K., *supra* note 28.
[33] Danielle Garno & Krithika Rajkumar, *supra* note 29.

domain, and the application of smart contracts on the blockchain to automatically enforce legal opinions without relying on physical-world authorities.[34]

XIII. XIII. WHAT FRAMEWORKS GOVERN THE METAVERSE?

At present, the metaverse is governed not by a self-contained legal order, but by the extension of existing legal frameworks developed for the physical world. Trademark disputes concerning brand identity, for example, continue to be governed by instruments such as the Lanham Act in the United States and the European Union Trade Mark Regulation in the European Union. Difficulties nonetheless arise when these frameworks are applied to virtual goods. Under the Nice Classification, physical goods such as handbags fall within Class 18, whereas NFTs and downloadable virtual goods are generally placed within Class 9. This has led many brand owners to seek separate trademark registrations specifically covering virtual goods and services. US courts have also relied on the *Rogers v. Grimaldi* test to balance trademark protection against claims of artistic expression under the First Amendment.[35]

Copyright law likewise remains central to disputes involving the unauthorised reproduction of digital artworks, virtual environments, and other protected material, with regimes such as the United States Copyright Act and the European Union's InfoSoc framework continuing to provide the principal legal basis. Consumer protection law has also begun to intersect more directly with intellectual property enforcement in response to digital fraud and deceptive online practices. In India, for instance, the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 impose obligations relating to transparency, grievance redressal, and platform responsibility. Private ordering also plays an important role. Platform terms of service frequently determine how intellectual property is owned, licensed, and used within virtual spaces, while smart contracts may embed licensing restrictions and transactional conditions directly into digital assets themselves.[36]

XIV. PREFERABLE LEGISLATION: NEW METAVERSE ACT, A DAWN OF A NEW LEGISLATIVE WORLD

[34] Bohadana Martins, *supra* note 26.

[35] Ananya Khandare, *supra* note 22.

[36] Moulika Sharma & Sanvi Mathur, *From Pixels to Prosecution: Tackling Crime in the Immersive Realms of Metaverse*, VI Sml. L. Rev. 220 220-52 (2023) https://www.hpnlu.ac.in/PDF/a7ef1747-02a4-4384-8104-82ff714e6d54.pdf [https://doi.org/10.70556/hpnlu-slr-v6-I1-2023-09].

A practicable legislative response would be the enactment of a dedicated Metaverse Act, designed to address the distinctive legal, commercial, and regulatory issues arising within immersive digital environments.

Article 1: Definitions and Legal Personhood

The metaverse shall be defined as an interactive, computer-generated three-dimensional ecosystem that integrates virtual and physical realities and enables users to participate through avatars. Avatars shall be recognised not merely as digital objects, but as externalised representations or digital delegates of their human users. Interference with an avatar's personal space may therefore, where appropriate, be treated as interference with the user's personhood. Digital assets, including non-fungible tokens and cryptocurrencies, shall be recognised as electronic records capable of exclusive control.[37]

Article 2: Personal Safety and Metaverse-Specific Offences

The law shall prohibit and criminalise serious forms of non-consensual conduct committed through avatars or immersive technologies. This includes metaverse-specific harms such as virtual sexual assault, persistent unwanted proximity after blocking, non-consensual avatar intrusion, and the creation or dissemination of sexually explicit AI-generated deepfakes of identifiable persons without consent. Such acts shall be treated as serious violations in light of their potential psychological and emotional consequences.

Article 3: Child Protection and Age-Appropriate Design

Digital service providers shall implement commercially reasonable age-verification measures to protect minors from harmful content. Platforms, app stores, and developers shall obtain parental consent where required before minors create accounts, download applications, or make in-app purchases. Age-appropriate design obligations shall include privacy-by-default settings, restrictions on manipulative design practices, and limits on precise geolocation tracking and automated profiling of children.[38]

---

[37] Clare McGlynn & Carlotta Rigotti, *From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse*, 45 Oxford J. Legal Stud. 554, 554-82 (2025), https://academic.oup.com/ojls/article/45/3/554/8108104 [https://doi.org/10.1093/ojls/gqaf009].

[38] Amber C. Thomson, et. al., *Little Users, Big Rules: Tracking Children's Privacy Legislation*, Mayer Brown (Jan. 28, 2026), https://www.mayerbrown.com/en/insights/publications/2026/01/little-users-big-rules-tracking-childrens-privacy-legislation [https://perma.cc/EU8N-AYFU] (last visited Apr. 11, 2026).

Article 4: Data Sovereignty and Biometric Privacy:

The collection and processing of sensitive biometric and body-based data, including eye-tracking, gait analysis, and brain-computer interface data, shall be subject to strict regulation. Such data may be processed only where strictly necessary and on the basis of clear and informed consent. Data minimisation requirements shall apply, and sensitive information collected for verification or access purposes shall not be retained or sold beyond what is strictly necessary.[39]

Article 5: Digital Commerce, Property, and Taxation

The law shall regulate virtual commerce, digital property, and taxation in order to promote market stability and prevent abuse. Existing financial rules concerning practices such as wash trading and insider trading may be extended to digital markets where appropriate. Smart contracts shall be enforceable only where the requirements of contract law, including offer, acceptance, and genuine consent, are satisfied. Virtual real estate shall be treated as a contractual asset or licensed interest governed principally by platform terms.[40]

Article 6: Commercial Liability and DAO Governance

Liability shall be allocated clearly among metaverse actors. Platform operators shall bear responsibility for system safety and for addressing unlawful content within their control. Individual users shall remain liable for fraud, abuse, or other unlawful conduct committed through their interactions. Entities deploying AI-controlled avatars or non-player characters shall bear responsibility for harmful conduct attributable to those systems. Decentralised autonomous organisations shall be required to adopt a legal structure capable of holding rights, assuming obligations, entering contracts, and bearing liability.[41]

Article 7: Interoperability and Anti-Monopoly Measures

The legislation shall promote interoperability and open standards in order to prevent dominant firms from creating closed and exclusionary digital ecosystems. Users shall, where feasible, be able to transfer their avatars and digital assets across platforms. Dominant metaverse platforms designated as

[39] *Metaverse Legal Frameworks*, Law & More (Jan 4, 2024), https://lawandmore.eu/blog/metaverse-legal-frameworks/ [https://perma.cc/M4F3-PZH5].
[40] Law & More, *supra note 40.*
[41] Jakub Jan Ziety & Rafal Pietraszuk, *A Few Remarks on the Legal Status of DAOs in the European Union and the Republic of Armenia*, 101 State and Law 16, 16-30 (2026) https://www.researchgate.net/publication/400445277 [https://doi.org/10.46991/SL/2025.101.016].

gatekeepers shall be prohibited from engaging in anti-competitive practices, including tying, unfair self-preferencing, and the combining of user data across services without clear consent.[42]

XV. CONCLUSION

The transition to a post-quantum digital civilisation marks a profound ontological shift and calls for a human-centred rethinking of legal, commercial, and educational institutions. The borderless structure of the metaverse and the expanding integration of generative artificial intelligence show the limits of applying analogue legal frameworks to decentralised digital realities. These limits are visible in the difficulty of regulating decentralised autonomous organisations, the growing need to extend trademark protection against digital forms of misappropriation, as illustrated by *Hermès v. Rothschild*, and the urgent need for a harmonised legal framework capable of protecting human identity against unauthorised synthetic replication.

The same structural dislocation is evident within academia. The increasing reliance on scientifically unreliable AI-detection tools, particularly those based on measures such as linguistic "perplexity" and "burstiness", has exposed serious epistemic, ethical, and pedagogical flaws. Such systems have not only produced false accusations against students but have also misclassified established literary works as AI-generated. A punitive model based on detection and discipline is therefore neither normatively defensible nor educationally sound.

A more credible response lies in developing an international, multi-stakeholder governance framework capable of addressing these transformations in a principled manner. Such a framework may draw upon robust human rights standards and other ethical traditions, including the justice-oriented principles associated with *maqasid al-Shariah*. The objective should be to create regulatory and institutional structures that preserve human agency, mental integrity, and fundamental rights, while enabling constructive forms of technological collaboration. The future of the metaverse and AI governance should therefore not be approached solely through reactive policing, but through a coherent legal order designed to ensure that technological progress remains accountable to human dignity and social justice.

[42] Int'l Bar Ass'n, Digital Regulations in the Metaverse Era: Europe, https://www.ibanet.org/document?id=Metaverse-project-Europe [https://perma.cc/6M3P-TTKC] (last visited Apr. 11, 2026).