https://doi.org/10.55843/SG2542101n

THE LEGAL ARCHITECTURE OF THE METAVERSE: PROPERTY, IDENTITY, AND VIRTUAL CRIME

Abdulatif Nuredini

ABSTRACT

The metaverse ecosystem, characterized by persistent, interactive, and often economically active virtual environments, simultaneously strains private law's property rights contract triangle, the digital extension of personality rights, and criminal law's architecture of legality, proof, and jurisdiction. This article systematically examines core legal issues in three axes: (i) virtual assets and claims of "virtual ownership," particularly NFT-based representations; (ii) digital identity and the legal protection of avatar-related harms; and (iii) virtual crime, with a focus on electronic evidence and cross-border jurisdiction. Treating the metaverse not merely as a technological novelty but as a normative friction zone between platform governance ("private ordering" through platform rules) and state law, the study combines doctrinal analysis, EU-anchored comparative inquiry, and a multi-case approach. The findings indicate that "virtual ownership" often functions not as classical property in rem, but as a bundle of rights (access, licensing, claims, token control, and account governance); that avatar-based harms make the digital dimension of personality rights particularly salient; and that, in virtual crime, the principal bottleneck frequently lies less in substantive definitions than in electronic evidence and transnational enforcement. The concluding section advances recommendations on conceptual clarity, grounding platform duties of care in positive law (notably the EU Digital Services Act), evidence preservation standards, and international cooperation.

Keywords: metaverse law; virtual assets; virtual ownership; NFTs; platform governance; digital identity; avatars; virtual harassment; electronic evidence; jurisdiction; comparative law; Digital Services Act (DSA).

Abdulatif Nuredini, Ph. D student
International VISION University, Gostivar

e-mail: abdulatif.nuredin@vision.edu.mk

UDK:
347.2:004.946(4-672EU)
343.3/.7:004.946(4-672EU)
159.923:004.946(4-672EU)

Declaration of interest: The authors reported no conflict of interest related to this article.

1. Introduction

The metaverse refers to shared digital spaces in which users interact through avatars, typically in persistent and multi-user settings. These environments have moved beyond gaming and communication: they now host virtual commodities, user-generated content economies, digital services, and new modes of identity performance. In blockchain-based implementations, "ownership" claims are articulated through NFTs and token representations, while platform terms of service (ToS) operate as a de facto body of private norms. As a result, metaverse disputes simultaneously generate uncertainty across private law (contracts, consumer protection, intellectual property), public law (data protection and market oversight), criminal law (legality and attribution), and cross-border dimensions (jurisdiction, applicable law, and mutual legal assistance).

This article adopts an EU-centered jurisdictional perspective for two reasons. First, the European Union has established a comprehensive framework for platform responsibility and content governance through the Digital Services Act (Regulation (EU) 2022/2065). Second, it has developed institutional tools for cross-border access to electronic evidence, notably the EU e-evidence package (Regulation (EU) 2023/1543 and Directive (EU) 2023/1544) and, more broadly, the Second Additional Protocol to the Budapest Convention (CETS No. 224). Because metaverse cases often turn on platform obligations and the practical feasibility of evidence access, the EU approach on these two axes provides directly usable analytical leverage.

Positioning within the literature. Metaverse scholarship frequently addresses virtual property, avatar harms, and virtual crime in separate tracks. This article seeks to integrate these strands by (i) operationalizing a bundle of rights classification for virtual assets via an analytical matrix (Table 1) and (ii) linking substantive criminal law questions to the procedural bottlenecks of electronic evidence and cross-border jurisdiction.

Contributions. The article makes three concrete contributions:

A bundle-of-rights matrix (Table 1) that maps metaverse disputes (token, service/access, account governance, IP, and reputation) to their core legal regimes.

A protection rationale for avatar-based harms grounded in the intersection of personality rights and data protection (including profile, behavioral, and potentially biometric data).

A criminal-procedure oriented proposal that centers on e-evidence (preservation/production), cross-border jurisdiction, and international cooperation (CETS No. 224 and the EU e-evidence package).

The article touches on competition law, securities/financial regulation, and taxation only to the extent necessary, focusing instead on three core questions: (1) under what conditions can NFT-represented virtual assets be protected analogously to objects of property rights; (2) how should avatar-related conduct (harassment, reputational attacks, identity theft) be addressed through personality rights and data protection; and (3) in virtual crime, is the decisive difficulty substantive legality or, rather, electronic evidence and cross-border jurisdiction?

Thesis: Because current law often attempts to reconstruct the metaverse triad of object, actor, and place by analogy, it produces systematic gaps in both private law and criminal procedure. An effective response requires a multi-layer model that classifies virtual assets as bundles of rights, incorporates platform governance into the regulatory equation, and recenters evidence and jurisdiction.

2. Methods and Materials

The study employs qualitative methods and combines three complementary approaches. First, doctrinal analysis reinterprets the concepts of property and rights, contractual allocation, intellectual property, personality rights, and the principle of legality in criminal law within the metaverse context. Here, Lawrence Lessig's "Code is Law" thesis provides the theoretical lens to explain the de facto regulatory power of platform architecture. Second, comparative analysis surveys selected jurisdictions, primarily the EU and the United States, focusing on virtual asset classification, platform responsibility, and access to electronic evidence. Third, a multi-case approach draws on reported dispute patterns in Decentraland, The Sandbox, and Horizon Worlds,

selected for economic intensity, user-generated content, governance model (centralized vs. on-chain), and diversity of dispute types.

Literature search strategy. The review covers 2004–2026, with particular attention to post-2019 NFT and metaverse scholarship. It draws on key law and law and technology databases (HeinOnline, Westlaw/LexisNexis, SSRN, Google Scholar) alongside EU primary and secondary sources (EUR-Lex; European Commission and ESMA materials). Search strings combined terms such as "metaverse law," "virtual property," "NFT legal nature," "platform liability," "Digital Services Act," "electronic evidence," "Budapest Convention Second Additional Protocol," "avatar harassment," and "identity in virtual worlds." Inclusion criteria required a direct legal argument on (i) virtual-asset classification or the token≠IP distinction, (ii) avatar/identity harms and personality/data protection, or (iii) electronic evidence and jurisdiction in criminal procedure. Technical-only descriptions without legal implications and low-reliability media content were excluded.

The comparative inquiry focused on five headings:

Platform responsibility and content governance (notice and action, transparency reporting, risk mitigation).

Consumer information duties and unfair terms control (unilateral changes and account termination).

Electronic evidence request and retention regimes (preservation/production; log retention).

Cross-border jurisdiction and mutual legal assistance (EU e-evidence package; CETS No. 224).

Regulatory context for crypto-assets (MiCA) and its points of contact with metaverse economies.

3. Theoretical Framework and Metaverse Typology

In the metaverse, state law is not the sole ordering force. Platform code can determine access conditions, economic mechanics, identity verification, sanctions, and even the production and availability of evidence, thereby performing a regulatory function. This generates tension at two levels: (i) platform rules create a de facto legal status for users (account termination, inventory revocation, content removal); and (ii) this private ordering may conflict with state law in consumer protection, data protection, and criminal investigations.

Accordingly, "one metaverse" should not be treated as a single analytical unit. For legal clarity, the metaverse can be categorized by:

Platform type: game-based, social VR, open-world, corporate metaverse.

Asset infrastructure: blockchain-based or non-blockchain (centralized database).

Asset type: on-chain tokens (NFT/FT), off-chain content, service/access rights, user-generated content (UGC).

Governance model: centralized moderation and contractual ordering vs. community governance and on-chain mechanisms.

Why the typology produces legal consequences. Each distinction triggers a different legal regime: (i) the blockchain/centralized split affects where evidence is generated and who controls it, shaping e-evidence access strategies; (ii) UGC intensity foregrounds IP law and notice-and-action procedures; (iii) service/access dominance makes consumer law, remedies for non-performance, and scrutiny of unilateral changes decisive; and (iv) governance models determine the platform's practical capacity for moderation, logging, and account sanctions thereby shaping the scope of any duty of care. Disputes should therefore be reduced first to the "core relationship" revealed by the typology and then connected to the appropriate legal regime.

4. Virtual Assets and NFTs: Not "Ownership" but a Bundle of Rights

NFTs technically record control over a unique on-chain token. In most cases, however, this record does not automatically transfer underlying intellectual property. (Delev, 2025) An NFT typically represents (i) token

control, (ii) platform-recognized access/display functionality, or (iii) a limited license signal. The assumption that "NFT owner = owner of the digital work" is therefore legally misleading.

This distinction has practical significance in consumer law. Market actors may frame token control as "full ownership," shaping user expectations. Where the token≠IP distinction is not disclosed with sufficient clarity, claims may arise based on misleading commercial practices, defective performance, or informational deficiencies. A transparent "bundle of rights disclosure" thus becomes a dispute reduction tool, not merely a conceptual refinement.

To resolve metaverse disputes, "ownership" should be decomposed into separable rights: on-chain token control, platform account/inventory governance, service/access rights, IP licensing, and claims against sellers or marketplaces. Table 1 operationalizes this decomposition, linking each rights type to core regimes, jurisdiction patterns, evidence management, and sample contractual clauses.

Table 1. Expanded Metaverse Dispute Matrix: Rights Type Regime Jurisdiction Evidence Clause

Virtual asset / right type	Dominant legal characterization (technical)	Primary risk / dispute	Core legal regime	Applicable law / jurisdiction (typical)	Typical evidence	Minimum evidence preservation	Suggested standard clause (summary)	Recommended pathway
Token control (NFT/FT)	On-chain record and disposition; IP transfer not automatic	Counterfeit collections; unauthorized transfers; misleading marketing; phishing	Contract + consumer law + tort (as applicable)	Consumer domicile/effects + platform/marketplace nexus; consider evidence location	On-chain transaction records; wallet signatures; marketplace logs	Transaction hash + timestamp; marketplace logs ≥ 6 months; hashed export at incident time	Explicit token≠IP statement; remedies for defect/misrepresentation; security incident notice	Marketplace duty of care; consumer remedies; interim relief + on-chain tracing
Account / inventory governance	Contractual allocation within platform; termination/revocation often reserved	Unjustified bans; asset revocation; arbitrary moderation; no appeal	Contract + unfair terms control + consumer law (where applicable)	ToS jurisdiction clauses vs. consumer protection/public policy; effects in user market	ToS; notices; moderation decisions; access logs	Ban/violation logs ≥ 6 months; reasoned decision with timestamped record	Reason-giving; appeal/ADR; limits on unilateral change; portability options	Transparent process; graduated sanctions; independent appeal/ADR; audit-ready records
Service/access rights (land/room/event)	Service/access contract; often time-limited license/subscription	Unilateral changes; event cancellation; access denial	Contract + consumer law + remedies for non-performance	Consumer domicile and targeted market; unfair terms review	Purchase/subscription records; platform announcements; payment records	Purchase record + change notices ≥ 2 years; dispute export capability	Unilateral change: prior notice, valid reason, free cancellation/refund	Standardization; refund/price reduction; temporary access remedy; transparent change policy

Service/access rights (land/room/event)	Service/access contract; often time-limited license/subscription	Unilateral changes; event cancellation; access denial	Contract + consumer law + remedies for non-performance	Consumer domicile and targeted market; unfair terms review	Purchase/subscription records; platform announcements; payment records	Purchase record + change notices ≥ 2 years; dispute export capability	Unilateral change: prior notice, valid reason, free cancellation/refund	Standardization; refund/price reduction; temporary access remedy; transparent change policy
User-generated content (UGC)	IP + license + platform notice-and-action policy	Copying; unauthorized use; abusive takedowns; repeat infringement	IP law + contract + notice-and-action obligations	Targeted country and right-holder nexus; platform establishment	Content hashes; upload history; takedown notices/counter-notices	Hash + timestamp; takedown file ≥ 6 months; repeat-infringer records	Notice-and-action + counter-notice; abuse sanctions; clear license scope	Rapid action with due process; repeat infringer sanctions; licensing clarity
Digital goods (skins/items)	License/access + inventory; secondary markets add	Misleading sales; secondary-market disputes; price manipulation	Consumer law + contract + tort (as applicable)	Consumer protection in targeted market; platform/marketplace nexus	Marketplace records; item descriptions; pricing history	Item page snapshot + transaction records; logs ≥ 6 months	Mandatory disclosure fields: access/license/transferability	Disclosure standard; refunds/ADR; market oversight and transparency
Reputation/identity (avatar)	Personality rights + data protection (profile/behavioral/potential biometric data)	Defamation; doxxing; identity theft; virtual harassment	Personality rights + data protection + platform rules	Effects-based: victim domicile/effects; controller/processor position	Content records; reports; communications logs; moderation decisions	Case file + logs ≥ 6 months; hashed incident captures	Complaint/appeal process; safety tools; risk-based verification; graduated sanctions	Fast removal/blocking; verification options; remedies + protective measures

Note: Table 1 is designed to move beyond the binary question "Are NFTs property?" by matching disputes to their core regime and evidence strategy based on where the issue concentrates.

At the comparative level, virtual goods also generate disputes in trademark and design law. Hermès International v. Rothschild (the "MetaBirkins" case) brought into focus the boundary between expressive/artistic uses of NFT representations and the source-indicating function of trademarks. The case is used here as an illustrative indicator that metaverse economies will be shaped not only by token technology,

but also by traditional IP enforcement and consumer-perception dynamics.

5. Digital Identity and Avatars: Personality Rights, Data Protection, and Platform Care

Avatars serve as interfaces for users' identity performance and social presence. The claim that avatar-based attacks—such as virtual harassment, persistent stalking, or reputational sabotage—do not generate "real harm" has been challenged in the literature. Because attachment to avatars can be linked to self-understanding, avatar-related harms may have moral and psychological effects. Accordingly, such conduct should not be treated exclusively as a breach of platform community rules; where warranted, it should also be assessed as an infringement of personality rights and/or as a violation of data protection norms.

Identity verification in the metaverse requires a delicate balance between anonymity and accountability. A one-size-fits-all "real name" mandate can be disproportionate in light of privacy and freedom of expression. A more viable approach is layered verification: users may remain pseudonymous by default, while risk-based checks apply to high-value transactions or repeated violations, and lawful identity disclosure remains available through due process for competent authorities (Nuredin; İnan, 2024).

Data-protection dimension. Avatar and identity data in metaverse settings are heterogeneous: profile data (usernames and account histories), behavioral data (movement and interaction patterns, social graphs), location data, and, particularly in VR/AR data that may acquire biometric characteristics (eye tracking, facial/body movement, voice). In the EU context, these datasets can fall within GDPR personal data and, depending

on circumstances, raise special-category risks. Risk-based verification may also conflict with privacy, freedom of expression, and data-minimization principles, requiring purpose limitation, minimal processing, and strong transparency and redress mechanisms.

Platform duty of care and positive law grounding (EU/DSA). Platform care obligations should be anchored in positive law rather (Nuredin; İnan, 2025) than treated as mere "good governance" In the EU, the Digital Services Act establishes a normative framework for content governance and transparency, encompassing notice and action procedures, justification for decisions, internal complaint and redress mechanisms, transparency reporting, and, particularly for very large online platforms, risk assessment and risk mitigation for systemic harm. Metaverse platforms, especially those with significant UGC and harassment risks, are likely to be shaped by these requirements through direct compliance logic. This article, therefore, argues for standardizing complaint review appeal workflows, establishing minimum log retention and evidence-preservation practices, and applying graduated sanctions for repeat violations as a "core adaptation" of DSA-aligned governance.

6. Virtual Crime: Evidence and Jurisdiction Before Substantive Labels

6.1. Legality and proportionality: new offenses or interpretive updates?

Fraud, threats, extortion, and unlawful acquisition of personal data generally map onto existing offense definitions across many legal systems. By contrast, concepts such as "virtual sexual harassment/contact" may expose gaps where statutory language presupposes physical contact. Two routes are plausible: clarifying that existing offenses encompass digital/virtual modalities through

interpretation or limited legislative updates, or adopting narrowly tailored provisions with objective thresholds such as persistent harassment and demonstrable serious psychological harm. In either case, legality and proportionality tests should be applied to mitigate risks to freedom of expression and privacy.

6.2. Electronic evidence: preservation, retention, rapid requests, and international cooperation

In practice, the dominant bottleneck is often not "what happened," but "how it can be proven." Platform logs, messaging records, transaction histories, on-chain transfers, and user captures (e.g., screen recordings) must be preserved with integrity, and their location and controllership determine whether and how they can be obtained. Metaverse-oriented criminal policy should therefore prioritize electronic evidence access, preservation mechanisms, and rapid request channels (Nuredin, 2025).

From an EU perspective, the European Production Order and European Preservation Order mechanisms under Regulation (EU) 2023/1543 are significant steps toward faster, more standardized cross-border access to electronic evidence. At the broader international level, the Second Additional Protocol to the Budapest Convention (CETS No. 224) strengthens cooperation for disclosure of electronic evidence, including enhanced channels involving service providers. These instruments do not eliminate the "where is the evidence?" problem, but they reduce loss of evidence risks by enabling preservation orders, standardizing request formats, and facilitating expedited cooperation for subscriber and access data where legally permitted.

Jurisdiction in metaverse cases is inherently multi-nodal: relevant links may include the actor's location, the victim's habitual residence, the platform's establishment, and the data storage location. Consequently, ToS-based jurisdiction clauses may conflict with consumer protection/public-policy limits, while criminal jurisdiction follows public law principles. This article proposes a three-step jurisdiction analysis: (i) classify the relationship (consumer, commercial, tort, or criminal); (ii) identify the locus of effects and the victim's connection; and (iii) assess evidence access realities based on platform data policies and available cooperation instruments.

7. Synthesis of Findings

The synthesis yields three principal conclusions. First, because metaverse "ownership" commonly operates as a bundle of rights rather than classical property, solutions should not be reduced to the binary question of whether NFTs are objects of property; rights type matching, as in Table 1, is more functional. Second, treating avatar harms as mere "in-game issues" obscures the digital extension of personality rights and the data protection dimension; effective protection flows from recognizing these rights in digital contexts and from enforceable platform duties of care. Third, in virtual crime, new offense creation is often less decisive than the workability of electronic evidence preservation and cross-border cooperation; the policy center of gravity should therefore shift toward evidence standards and rapid request mechanisms.

8. Conclusions and Recommendations

The metaverse is not only a new domain of application; through platform governance, it changes how norms are practically applied. Effective responses should connect recommendations through a matrix logic: problem area (property/identity/crime) → tool (definitions, platform

duties, evidence standards) → actor (legislator/courts/platforms/international mechanisms) → expected impact (reduced uncertainty, improved proof, user protection).

Table 2. Recommendations Matrix: Problem → Tool → Actor → Expected Impact

Problem area	Tool	Actor	Expected impact
Virtual assets / "ownership" claims	Legal definition + bundle-of-rights disclosure; consumer information and unfair terms control	Legislator (definitions); platforms/marketplaces (disclosure); courts (legal characterization)	Less misleading marketing; correct regime matching; fewer disputes
Avatar/identity harms	Standardized complaint–appeal workflows; risk-based verification; data minimization + transparency	Platforms (implementation); regulators (compliance); courts (personality/data protection)	Faster protection; fewer repeat harms; better rights balancing
Virtual crime / e-evidence	Preservation/production standards; log retention and formats	Law enforcement/courts (requests); platforms	Reduced evidence loss; more effective

	(hash/timestamp); rapid request channels	(retention/production); international cooperation bodies	cross-border investigations

Accordingly, four consolidated recommendations follow:

Conceptual clarity: define "virtual assets" and subtypes in relevant legal instruments; require disclosure of token control vs. license vs. access in consumer-facing interfaces.

Platform duty of care: require standardized complaint and appeal processes, reasoning, transparency reporting, and minimum log retention in a DSA-aligned governance model.

Electronic-evidence centered criminal procedure: prioritize preservation, standardized formats (hash/timestamp), rapid requests, and cross-border cooperation (EU e-evidence package and CETS No. 224).

Education and expertise: strengthen curricula and professional training in digital law, platform governance, blockchain, and electronic evidence for legal practitioners and authorities.

References

Ali, O., Momin, M., Shrestha, A., Das, R., Alhajj, F., & Dwivedi, Y. K. (2023). A review of the key challenges of non-fungible tokens. Technological Forecasting and Social Change, 187, 122248. https://doi.org/10.1016/j.techfore.2022.122248

Balkin, J. M. (2005). Law and liberty in virtual worlds. New York Law School Law Review, 49(1), 63–80.

Brittain, B. (2024, October 23). MetaBirkins NFT creator, Hermès square off in U.S. trademark appeal. Reuters.

Chohan, U. W. (2021). Non-fungible tokens (NFTs): Early thoughts and a research agenda. Critical Blockchain Research Initiative (CBRI) Working Paper. https://doi.org/10.2139/ssrn.3822743

Council of Europe. (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

Delev, Jordan. (2025). New Trends in the Development of EU Intellectual Property Law: Design Reform. III International Symposium on Current Developments in Intellectual Property Law – Full Text Proceedings Book. Ed. Canan KÜÇÜKALİ, Mustafa YASAN, Aytuğ Ceyhun ÇAKIR. Filiz Kitabevi. Istanbul, Türkiye. 112-130.

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. (2023). Official Journal of the European Union.

European Commission. (n.d.). Digital Services Act.

European Securities and Markets Authority. (n.d.). Markets in Crypto-assets Regulation (MiCA).

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union.

European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union.

European Union. (2023). Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European production orders and European preservation orders for electronic evidence. Official Journal of the European Union.

European Union. (2023). Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets. Official Journal of the European Union.

Fairfield, J. A. T. (2005). Virtual property. Boston University Law Review, 85(4), 1047–1102.

Hermès International v. Rothschild, No. 1:22-cv-00384 (S.D.N.Y. 2023).

Kerr, O. S. (2008). Criminal law in virtual worlds. University of Chicago Legal Forum, 2008(1), 415–429.

Lastowka, F. G., & Hunter, D. (2004). The laws of the virtual worlds. California Law Review, 92(1), 1–73. https://doi.org/10.2307/3481444

Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.

Wolfendale, J. (2007). My avatar, my self: Virtual harm and attachment. Ethics and Information Technology, 9(2), 111–119. https://doi.org/10.1007/s10676-006-9124-6

Nuredin, A., & İnan, T. C. (2025, January). International criminal law in the metaverse: Digital adaptation for crimes against humanity. In *Proceedings of the International Symposium on Law, Justice, and Emerging Global Challenges* (pp. 233-244).

Nuredin, A., & İnan, T. C. (2024). Cyber warfare and international criminal law: State responsibility for cyber attacks. In *International Scientific Conference on AI, Human Rights, Migration, Democracy, and Public Impact* (pp. 188-200).

Nuredin, A. (2025). *Uluslararası Kamu hukuku* (pp.850). International Vision University.