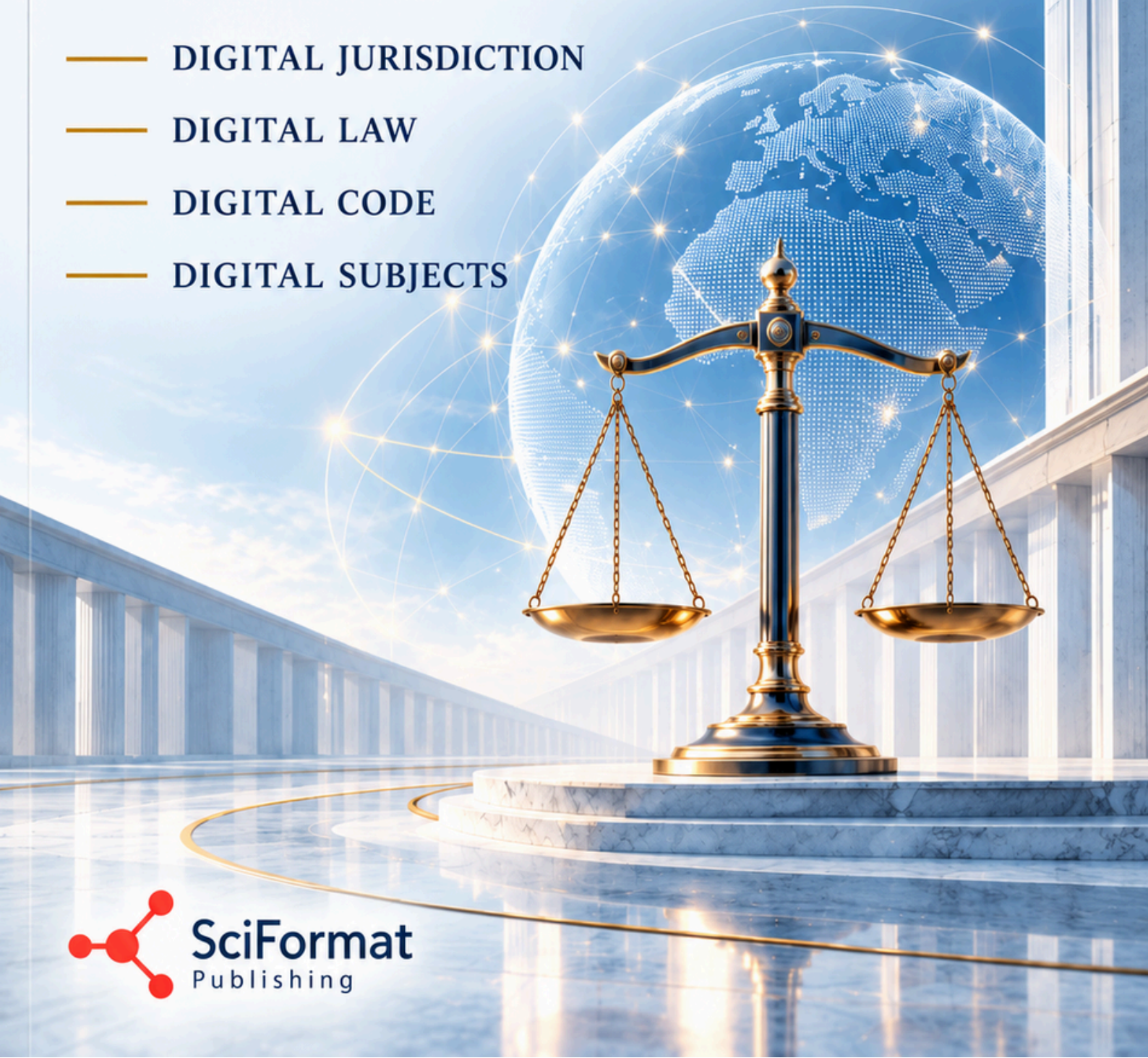
Metaverse and Digital Law

Oleksii Kostenko

- DIGITAL JURISDICTION
- DIGITAL LAW
- DIGITAL CODE
- DIGITAL SUBJECTS



SciFormat Publishing

Oleksii Kostenko

METAVERSE AND DIGITAL LAW

DIGITAL JURISDICTION
DIGITAL LAW
DIGITAL CODE
DIGITAL SUBJECTS

MONOGRAPH

Canada, 2026

Metaverse and Digital Law

Oleksii Kostenko

Published by **SciFormat Publishing Inc.** | Canada | 2026

ISBN: 978-1-0690482-6-4 (eBook) **DOI:** 10.69635/978-1-0690482-6-4

Suggested citation: Kostenko, O. V. (2026). *Metaverse and Digital Law*. SciFormat Publishing Inc.

Peer reviewers

D. V. Zhuravlev, Doctor of Law, Professor, Honored Lawyer of Ukraine, Deputy Head of the Department for Citizenship, Pardons, State Awards – Head of the Department for Pardons of the Office of the President of Ukraine.

N. M. Onishchenko, Doctor of Law, Professor, Honored Lawyer of Ukraine, Academician of the National Academy of Legal Sciences of Ukraine, Deputy Director for Research of the V.M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine.

Abstract

The monograph is devoted to the formation of a new legal architecture for digital civilisation, within which the Metaverse, Web 4.0, artificial intelligence, blockchain, decentralised autonomous organisations and digital twins cease to be merely technological phenomena and become a fully developed environment for the emergence of social relations, legal conflicts, rights, obligations and liability.

For the first time, the study proposes an integrated set of original models of digital jurisdiction, digital law, the Digital Code and digital subjects. Digital jurisdiction is substantiated as a post-territorial form of organising legal space, capable of operating within cross-border, decentralised and algorithmically governed ecosystems. Digital law is considered not as a mechanical extension of information law, but as a comprehensive system for regulating relations arising among natural persons, platforms, algorithmic agents, autonomous artificial intelligence systems, digital persons, avatars and other digital subjects.

Particular attention is devoted to the author's model of the Digital Code — a modular, technologically neutral and adaptive instrument for the systemic regulation of digital ecosystems. The monograph also presents a model Digital Criminal Code and examines the legal nature of digital identity, virtual assets, decentralised autonomous organisations, digital twins, algorithmic liability and automated governance.

The study combines philosophical and legal analysis with applied regulatory constructs and offers a coherent methodology for moving from the fragmented regulation of individual technologies towards the establishment of a new legal order for digital reality.

The publication is intended for scholars, legal professionals, legislators, civil servants, digital policy specialists, experts in artificial intelligence, and students and researchers in higher education.

© 2026 Oleksii Kostenko. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

Licence: https://creativecommons.org/licenses/by/4.0/

Certificate of registration of the Austrian right to the work No. 150728 dated 08.09.2026.

TABLE OF CONTENTS

LIST OF CONDITIONAL ABBREVIATIONS 8

CHAPTER 1. THEORETICAL, METHODOLOGICAL AND CONCEPTUAL FOUNDATIONS OF METAVERSE LAW 12

1.1. Theoretical and methodological foundations of the formation of the conceptual and categorical apparatus of Metaverse law 12

1.1.1. Terminology. 17

1.1.2. Differentiation of the Metaverse from related categories and working definition. 22

1.1.3. Metaverse Objects: Typology and Legally Relevant Attributes. 23

1.2. Metaverse as an object of legal regulation: structural and functional characteristics, life cycle and interaction 24

1.2.1. Features of the Metaverse as an object of normalisation. 25

1.2.2. Phases of development of Metaverse platforms and the evolution of regulatory regulation of digital ecosystems. 26

1.2.3. Methodology for periodisation of Metaverse platforms. 26

1.2.4.Web 1.0-3.0 as a prerequisite for the Metaverse. 29

1.3. Web 4.0\Metaverse Concept in the European Union: Regulatory Vectors, Standards, and Regulatory Approaches 31

1.3.1. Web 4.0\Metaverse Concept and European Union 31

1.3.2. The regulatory trajectory of the Metaverse in the EU strategy. 35

1.3.5. PRC and Metaverse. 43

1.4. Metaverse Architecture as a Subject of Legal Analysis: Correlation of Technical Layers to Legal Regimes 48

1.4.1. Metaverse Architecture 48

1.4.2. The principle of legal stratification: "layers" of infrastructure and regimes of law. 52

1.4.3. Digital identity and attribution layer. 55

1.4.4. Data layer: privacy, cybersecurity, logging. 59

1.4.5. Content and behaviour layer: moderation, responsibility, IP. 62

1.4.6. Transactional-economic layer. 65

1.4.7. Evidence (audit) layer. 68

1.4.8. Layer of sanctions and their application. 71

1.4.9. Multi-Level Trust, Compliance, and Risk Management in the Metaverse. 71

1.4.10. The genesis of the legal regulation of the Metaverse. 74

1.4.11. Formation of the concept of "information society". 75

1.4.12. Methodology of Legal Regulation of Web 2.0 81

1.4.13. Metaverse Structure Based on Web 3.0 Technologies 84
1.4.14. Problems of Legal Regulation of Public Relations in Web 2.0-Web 3.0 89
1.4.15. Subjects of legal relations in Web 2.0-Web 3.0. 91
1.4.16. Objects of Legal Regulation in Web 2.0-Web 3.0. 94
1.4.17. Legal procedures Web 2.0-Web 3.0. 97
1.4.18. Responsibility in Web 2.0. 100
1.4.20. Proof in Web 2.0-Web 3.0. 102
1.4.21. Cross-border and conflict issues Web 2.0-Web 3.0. 104
1.4.22. Problems of legal regulation of the Metaverse. 107
CHAPTER 2. TECHNOLOGICAL, ETHICAL, AND LEGAL DETERMINANTS OF THE METAVERSE. **115**
2.1. Web 4.0 as a technological basis for the formation of legal relations in the Metaverse: theoretical and legal analysis 115
2.1.1. Artificial Intelligence as a Core Component of Web 4.0. 115
2.1.2. Epistemological limits of artificial intelligence. 116
2.1.4. Human Rights, Ethics, and Social Effects of AI 119
2.1.5. Military AI. 120
2.1.6. Regulation of AI through the prism of international human rights law. 123
2.1.7. Artificial intelligence strategies. 125
2.1.8. Problems of morality of autonomous artificial intelligence. 134
2.2. Internet of Things in the Metaverse Structure: Legal Aspects of Integration of Physical and Virtual Environments 140
2.2.1. Internet of Things 140
2.2.2. Metaverse Blockchain (DLT): A "Trust Space" for Digital Jurisdictions. 145
2.2.3. DTL-Metaverse matrix. 147
2.2.4. Blockchain in the Metaverse: Architecture and Legal Ontology. 149
2.2.5. Blockchain - Ukrainian context. 151
2.2.6. Blockchain, IoT and AI - the basis of digital jurisdiction. 156
2.3. Decentralized Autonomous Organizations (DAOs) as the Newest Form of Digital Self-Government: Legal Nature and Functions 159
2.3.1. Decentralized Autonomous Organization (DAO) in the classical sense 159
2.3.2. The legal nature of the DAO. 160
2.3.3. Legal personality and legal responsibility of the DAO. 162
2.3.4. Regulation of DAOs in the United States. 163
2.3.5. Regulation of DAOs in the European Union. 164
2.3.6. DAO as a tool for algorithmic compliance. 166

2.3.7. Five-Tier DAO Architecture for the Metaverse. 167
2.3.8. Functionality of DAOs in public administration of Ukraine. 173
2.4. Digital twins in the Metaverse: legal regime and features of use 177
2.4.1. Digital Twins. 177
2.4.2. Metaverse as a Cyber Physical-Social Paradigm Digital Twins. 179
2.4.3. Web3-oriented Metaverse architecture. 180
2.4.4. Industrial Metaverse and environmental dimension. 181
2.4.5. Social and behavioural aspects of digital twins. 182
CHAPTER 3. LEGAL REGIMES OF CONTENT, ASSETS, AND SUBJECTIVITY IN THE METAVERSE 183
3.1. Identity and Digital Identity as Objects of Legal Regulation in the Metaverse 183
3.1.1. Identification of subjects and objects in digital systems. 183
3.1.2. Legal aspects of identity management. 190
3.1.3. Cross-border three-level subject-object paradigm of management of identification 192
3.1.5. Secure and Confidential Metaverse Authentication Scheme. 195
3.1.6. Digital Metaverse Entities, Concept and Categorization. 197
3.1.7. Digital Actors' Rights: Basic, Delegated and Simulated. 199
3.1.8. Responsibilities and ethical standards of digital actors. 202
3.1.9. Varieties of digital subjects. 204
3.1.9.1. Avatars as interface subjects of the Metaverse. 205
3.1.9.2. Digital personalities as carriers of digital identity. 207
3.1.9.3. Digital humanoids and robotic agents as subjects of the Metaverse. 210
3.1.9.4. *Artificial intelligence systems with corporate rights.* 211
3.1.9.6. Artificial moral agents. 213
3.1.9.7. Digital (virtual) influencers. 215
3.1.9.8. Simulacrum as a standalone digital entity without a physical original. 217
3.2. Blockchain as an Institutional and Legal Infrastructure of the Metaverse: Ensuring Trust and Transparency 219
3.2.1. Briefly about blockchain 219
3.2.2. Blockchain in the Metaverse legal relationship system. 221
3.2.3.Conceptual and terminological framework of cryptocurrencies in the Metaverse. 224
3.2.4. The Legal Nature of Transactions with Cryptocurrencies in the Metaverse. 226
3.2.5. Metaverse Crypto Economy. 228
3.2.6. Jurisdictional Issues of Cryptocurrency Regulation in the Metaverse 235

3.3. Ownership in the Metaverse: Doctrinal Approaches and Regulatory Regulation of Virtual Objects and Tokenized Assets 237
3.3.1. Issues of Ownership and Intellectual Property in the Metaverse 237
3.4. Digital Legal Personality in the Metaverse: Models and Features of Implementation 245
3.4.1. Algorithmic legal capacity and delegated subjectivity. 245
3.4.2.Registration, identification and coding of digital entities. 246
3.4.3. Normative modes of delegation of authority. 248
3.4.4.Control, audit and recall of digital subjectivity. 250
3.4.7. The ethical and legal foundation of the Metaverse. 255
CHAPTER 4. METAVERSE: PRIORITIES FOR THE DEVELOPMENT OF A NEW PHILOSOPHY OF DIGITAL ENVIRONMENTS (AUTHOR'S APPROACH) 256
4.1. Methodological and philosophical foundations of the formation of the author's concept of Metaverse law 256
4.2. Transformation of the Philosophical and Legal Paradigm in the Metaverse: Author's Approach 257
4.2.1. The concept 257
4.2.2. The need for a new philosophy. 258
4.2.3. Philosophical Concepts of the Metaverse: Cosmology, Coevolution, Proto-Metaverse. 258
4.2.4. Metaverse Coevolution. 261
4.2.5. Proto-Metaverse. 263
4.3. Post-tropocentrism as a principle of legal understanding of the Metaverse. 268
4.3.1 Philosophic vectors. 268
4.3.2. Post-Anthropocentrism and Information Law. 271
4.3.3. Metaverse Philosophy and Digital Jurisdiction of Integrated Reality. 274
4.4. Metaverse as a Phenomenon of Metareality: The Author's Philosophical and Legal Interpretation 277
4.4.1. Ten main postulates of Metaverse philosophy. 277
4.4.2. The basis of the new philosophy of the Metaverse. 280
4.4.3. Metaverse Philosophy – Synthesis of Metareality Theories 282
CHAPTER 5. MODELS OF DIGITAL JURISDICTION AND DIGITAL CODE (AUTHOR'S APPROACH) 284
5.1. Conceptual and categorical foundations of digital jurisdiction (author's approach) 284
5.1.1. Definitions 284
5.1.2.The term "Metaverse". 285
5.1.3. The term "digital" and "electronic". 288

5.2. Digital jurisdiction as a post-territorial legal construction: theoretical and legal justification 294
5.2.1. Modern paradigms of legal regulation. 294
5.2.2 Code as the Constitution of Cyberspace: From Lessig to the Architecture of Digital Jurisdiction. 295
5.2.3. The End of the Peace of Westphalia: Law in the Age of Protocols and Platforms. 298
5.3. Digital Jurisdiction Model in the Metaverse Environment: Structural and Functional Analysis 300
5.4. Mechanisms for the implementation of digital jurisdiction in the context of the development of the Metaverse 306
5.4.1.Mechanisms for the legal regulation of social relations in the Metaverse 306
5.4.2. Principles of functioning of digital jurisdiction. 312
5.4.3. Key categories of digital jurisdiction. 315
5.4.4. Legal architecture of digital jurisdiction. 319
5.4.5. Regulatory mechanisms. 323
5.4.6. Cross-border regime of digital jurisdiction. 326
5.4.7. Responsibility in Digital Jurisdiction. 329
5.5. The concept of the Metaverse Digital Code: theoretical and legal foundations 329
5.5.1. Key functional elements 329
5.5.3. Theoretical foundations of the digital code model 332
5.5.6. Digital Code Modules 335
5.6. Theoretical and Legal Model of the Digital Criminal Code for the Metaverse. 347
5.7. Strategic Directions of Ukraine's Integration into the Digital and Legal Space of the European Union Web 4.0: Regulatory Foresight 351
5.7.1. The strategy of Ukraine's digital integration into the legal space of the European Union 351
5.7.2. Strategic recommendations in the field of rule-making and codification 353
5.7.3. Strategic Recommendations in the Field of Institutional Architecture 354
5.7.4. Legal mechanisms of Ukraine's integration into the EU digital space 356
AFTERWORD **360**
Legal Typologies of Metaverse, DLT and AI Governance **364**

LIST OF CONDITIONAL ABBREVIATIONS

Abbreviations	Full name
AML-CFT	Anti-Money Laundering / Counter-Financing of Terrorism
AI	Artificial Intelligence
AAI	Artificial Augmented Intelligence
ASI	Artificial Superintelligence
AR	Augmented Reality
VR	Virtual Reality
XR	Extended Reality
NFT	Non-Fungible Token
DLT	Distributed Ledger Technology
DAO	Decentralized Autonomous Organization
DeFi	Decentralized Finance
DID	Decentralized Identifier
KYC	Know Your Customer
WIPO	World Intellectual Property Organization
IEEE	Institute of Electrical and Electronics Engineers
ITU	International Telecommunication Union
WEF	World Economic Forum
OECD	Organisation for Economic Co-operation and Development
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework
TCP/IP	Transmission Control Protocol / Internet Protocol
ODR	Online Dispute Resolution
MNO	Mobile Network Operator
EPRS	European Parliamentary

Abbreviations	Full name
	Research Service
MiCA	Markets in Crypto-Assets Regulation
FG-MV-SI	Focus Group on Metaverse – Standardization Initiative (ITU)
MCE (ITU)	Metaverse Communication Environment
B2B	Business-to-Business
B2C	Business-to-Consumer
PIPL	Personal Information Protection Law
CAC	Cyberspace Administration of China
VETA	Virtual Economy and Token Assets
BJM	Business Judgment Model
WEB	World Wide Web

PREFACE

Aim and Scope

The development of immersive technologies, decentralised networks, and artificial intelligence systems has confronted legal scholarship with a challenge that extends beyond the conventional task of adapting law to new technology. The Metaverse, Web 4.0, decentralised autonomous organisations, and algorithmic agents together constitute an environment in which the foundational premises of classical law — the human being as the sole bearer of legally significant will, territory as the basis of jurisdiction, and centralised institutions as the source of enforcement — no longer hold universally.

This book offers a comprehensive theoretical-legal model for the regulation of this environment. Unlike existing studies, which largely focus on discrete aspects of the digital domain — personal data protection, electronic trust services, or the regulation of crypto-assets — the present work treats Web 4.0/Metaverse as a single, autonomous subject of legal analysis and proposes a coherent conceptual, doctrinal, and institutional apparatus for its regulation.

The aim of the study is to develop the theoretical and methodological foundations for the legal regime of Web 4.0/Metaverse technologies and to formulate a doctrine of digital jurisdiction as a foundational category for a new stage in the development of information law.

Structure and Content

The book is organised according to a principle of sequential development: from an analysis of technological premises, to the formulation of doctrine, and finally to institutional and codification models.

Technological premises. The role of key technological components in the formation of new legal relations is analysed separately: the Internet of Things as an integrative infrastructure connecting physical and digital environments; decentralised autonomous organisations as a new form of digital self-governance; digital twins as autonomous objects of legal regulation; blockchain as an institutional-legal infrastructure of trust; and artificial intelligence systems performing functions of algorithmic ranking, moderation, risk-scoring, and automated sanctioning.

Subject composition. A comprehensive classification of Metaverse subjects is proposed, encompassing eight categories of participants that have no counterpart in classical legal-subject theory: platform operators, decentralised autonomous organisations, infrastructure providers, digital personas, avatars, algorithmic agents, autonomous artificial intelligence systems, and digital twins. The legal personhood of each category is determined not by an anthropocentric criterion, but by a functional and delegated principle.

The doctrine of digital jurisdiction. The book's central section is devoted to substantiating digital jurisdiction as an autonomous, post-territorial legal institution. The doctrine is structured around six modules — normative, institutional, procedural, evidentiary, sanctions, and cross-border — and is supplemented by a system of legal anchors (provenance, infrastructural, identification, economic, and protocol-based) that enable the technological localisation of legally significant acts without recourse to the territorial principle.

A model of digital law and codification instruments. A theoretical model of digital law is developed as a comprehensive, cross-sectoral legal system with its own subject matter, method, and sources — among which code-based regulation is included for the first time: software code, algorithms, and smart contracts as an autonomous form of normative regulation. On this basis, a model of a digital code is constructed — a modular, technologically neutral codification system that permits phased implementation without the need for periodic wholesale revision. A model digital criminal code is presented separately, describing offences specific to immersive environments: fraud involving virtual assets, cyberstalking, and manipulative attacks based on synthesised content.

Foresight and preventive regulation. The book substantiates the concept of preventive digital rulemaking, combining doctrinal forecasting, experimental regulatory regimes, and institutional mechanisms of legal foresight aimed at the anticipatory formation of normative frameworks prior to the large-scale deployment of new technological solutions.

Philosophical-legal foundations. A separate section is devoted to the philosophical substantiation of the proposed models — a question that has been largely absent from the existing literature on Metaverse law. A philosophy of Meta-reality is developed as a synthesis of critical rationalism, process philosophy, and the thesis that "code is law," providing the methodological foundation for understanding Metaverse law as a dynamic rather than a static system. On this basis, a system of postulates for a theory of law in the Metaverse is formulated, together with a critical analysis of the risks inherent in immersive environments — algorithmic discrimination, the illusion of free choice, and alienation from physical reality.

Key Features of This Volume

For the first time, a comprehensive, interdisciplinarily coherent doctrine of the legal regulation of Web 4.0/Metaverse is proposed as an autonomous socio-technological environment.

For the first time, the concept of digital jurisdiction is substantiated as a post-territorial legal institution with a fully developed modular architecture.

For the first time, a comprehensive classification of digital-environment subjects is proposed, extending beyond the anthropocentric model of law.

For the first time, a model digital code and a model digital criminal code are developed as codification instruments of a new generation.

For the first time, a philosophical foundation for the legal regulation of the Metaverse is provided through interdisciplinary synthesis.

Twenty-two original definitions form a coherent conceptual-categorical apparatus suitable for further use in scholarly research and legislative practice.

Readership

This volume is addressed to researchers in information law, digital law, and comparative law; specialists in the regulation of emerging technologies; representatives of public authorities and regulatory institutions; faculty and postgraduate students in legal studies; and practising lawyers working on issues of digital assets, artificial intelligence, and immersive technologies. It will be of value to readers seeking a systematic understanding of the legal challenges posed by the digital environment, rather than an account limited to its individual manifestations.

CHAPTER 1. THEORETICAL, METHODOLOGICAL AND CONCEPTUAL FOUNDATIONS OF METAVERSE LAW

1.1. Theoretical and methodological foundations of the formation of the conceptual and categorical apparatus of Metaverse law

The theoretical and methodological basis of the study is the scientific developments of domestic and foreign scientists devoted to the above-mentioned problems of legal regulation of digital ecosystems, immersion technologies and algorithmic systems. At the same time, it should be noted that in the Ukrainian scientific space, the development of the outlined problems is mainly fragmentary, "point" in nature, which is objectively determined by a number of interrelated factors.

First of all, the full-scale armed aggression of the Russian Federation against Ukraine has significantly transformed the priorities of scientific policy and research programs, reorienting a significant part of the academic community to tasks directly related to ensuring the defence capability of the state, the stability of critical infrastructure and the preservation of human potential. Under such conditions, research that requires long-term interdisciplinary synthesis (law — engineering — ethics — security) often recedes into the background, giving way to the applied and immediate needs of law enforcement and risk management. An additional explanatory factor is the interdisciplinary nature of the relevant technologies and legal institutions: the combination of digital identity, virtual assets, platform governance, electronic evidence, algorithmic transparency and digital self-government models necessitates a comprehensive methodology capable of integrating the norms of public and private law with the technological parameters of the functioning of environments. In view of the above, the limitations of systematic research in the national context are situational structural and resource in nature.

In the global scientific discourse, the problems of the Metaverse and related digital ecosystems are distinctly active and cumulative: over the past five years, it has moved from predominantly technical descriptions to complex interdisciplinary studies in which legal regulation (regulatory regimes of data, digital identity, content, transactions, evidence, and sanctions) is considered as a necessary condition for the sustainable development of immersion media.

Empirical confirmation of this dynamics is bibliometric and scientometric works, which record a noticeable acceleration in the number of publications after 2020–2021, in particular in the direction of "Metaverse-based environments" and related topics (XR/VR/AR, digital twins, smart cities, platform models of interaction). Thus, some bibliometric reviews directly indicate a "sharp increase" in publications after 2020, as well as an acceleration of "Metaverse literature" since 2021 with a peak in the number of works in 2024 (Mutlu Avinc & Yildiz, 2025)[1].

For the first time in domestic legal science, a comprehensive systematic study of the theoretical and legal foundations of ensuring the legal regime of information technologies

1 Mutlu Avinç, G., & Yıldız, A. (2024). A bibliometric and systematic review of scientific publications on metaverse research in architecture: Web of Science (WoS*). International Journal of Technology and Design Education, 34*(2), 1–28. https://doi.org/10.1007/s10798-024-09918-1

Web 4.0/Metaverse has been carried out. Despite the active international discourse in the areas of platform regulation, data protection, AI governance, and e-justice, these lines of research often develop in isolation — without integration into a single legal model capable of embracing Web 4.0/Metaverse as a holistic socio-technological environment. It is this systemic gap that determines the relevance of the study.

A critical analysis of modern approaches shows that the problem is not the lack of research, but the conceptual disunity of the subject: the Metaverse is mostly explored as a socio-technological environment, while Web 4.0 is studied as an infrastructural-normative model of digital development. Such a dichotomy does not reflect the real nature of the phenomenon in question and complicates the formation of systemic legal regulation.

A question that remains debatable in the scientific literature requires special attention: are Metaverse and Web 4.0 two different phenomena — or are they two names of the same thing? The answer offered by this study is fundamentally important, not only in the terminological but also in the legal philosophical dimension. Metaverse is a concept of American origin, introduced into scientific and technological circulation long before the emergence of an appropriate regulatory framework. Web 4.0 is a European Union term introduced by Commission Communication COM/2023/442: the EU deliberately avoids American terminology, preferring its own definitions that reflect European values and regulatory philosophy. The Commission explicitly abandoned the term "Metaverse" in favour of "virtual worlds" and "Web 4.0" — not because it describes a different phenomenon, but because it describes the same phenomenon in a different way: through the prism of technological neutrality, human rights, and public values.

In this regard, the essence of the scientific problem lies in the absence of a holistic theoretical and legal concept that integrates Metaverse and Web 4.0 into a single subject of legal research and provides an adequate normative understanding of the new digital reality within the framework of information law.

Despite the fact that the title and content of the study formally indicate two objects — Metaverse and Web 4.0, the paper substantiates that they do not form two independent subjects, but constitute a single conceptual construct that exists in two interrelated dimensions: content (socio-economic and anthropological), reflecting digital reality as an environment of new legal relations; normative-architectural (legal and technological), which determines the mechanisms of its organisation and regulation.

This approach allows us to consider Metaverse and Web 4.0 as two projections of the same polystructural sociotechnical phenomenon, which have relative independence, but are not able to function in isolation.

Thus, Metaverse and Web 4.0 are not two independent subjects of legal regulation and are not just synonyms. These are two projections of the same civilisational phenomenon in different coordinate systems: the American framework describes it through the prism of an immersive environment and new forms of social reality, the European framework describes it through the prism of technological architecture and normative order. Just as in the legal doctrine the concepts of "entrepreneurial activity" and "economic activity" describe the same phenomenon with different accents, while maintaining an independent doctrinal meaning, so Metaverse and Web 4.0 are two components of a single subject of research, each of which cannot function without the

other: Web 4.0 without Metaverse is only a technical protocol without social and legal content; Metaverse without Web 4.0 is just a concept without an infrastructure framework. That is why the subject of this study is unique — but dual in nature.

We draw attention to an important aspect – the fundamental difference and unity of Metaverse and Web 4.0. On 11 July 2023, the European Commission adopted a new strategy on Web 4.0 and virtual worlds, aimed at ensuring an open, secure, trustworthy, fair and inclusive digital environment for EU citizens, businesses and public administrations; The strategy is in line with the goals of the Digital Decade program for 2030 and its three key areas: skills, business and public services.

In the legal dimension, it is fundamentally important that Web 4.0 is only a technological substructure of a broader phenomenon — the Metaverse: the former describes the architecture of the next generation of the Internet, while the Metaverse constitutes a full-fledged socio-legal reality, including Web 4.0 as a necessary but insufficient condition, and additionally encompasses new forms of social relations, specific subjects of law, digital identity and cross-border digital jurisdiction.

It is this conceptual difference — between technological (Web 4.0) and civilisational (Metaverse) — that defines the scientific problem of the dissertation research: the traditional legal categories of jurisdiction, legal personality, property and responsibility, developed in the era of analog and early digital law, are insufficient to regulate the social relations arising in the Metaverse. The Commission itself, having deliberately abandoned the term "Metaverse" in favour of "virtual worlds" (due to its non-European ontological origin), emphasised the value-oriented and technology-neutral nature of regulation.

The convergence of artificial intelligence, augmented and mixed reality, blockchain architectures, the semantic Internet, and "digital twin" technologies is shaping a qualitatively new human habitat — the Metaverse — within which traditional legal categories developed in the era of analog and early digital law are undergoing a systemic reassessment.

Fundamentally important for this study is a clear conceptual distinction between the concepts of *Web 4.0* and *Metaverse* — a distinction that has not only terminological but also deep legal and philosophical and regulatory significance.

Web 4.0 should be understood as *the technological-architectural* paradigm of the next generation of the Internet: a semantically enriched, AI-native, interoperable network, where digital objects seamlessly integrate with the physical environment, and interaction between humans and machines reaches the level of cognitive and sensory fusion. The European Commission itself, in its official Communication, defines Web 4.0 as the next step after Web 3.0, which "will allow the integration of digital and real objects and environments, as well as enhanced interaction between humans and machines" is a leap that creates a "seamlessly interconnected, intelligent and immersive world" (European Commission, 2023a)[1].

On 11 July 2023, the Commission adopted a new strategy on Web 4.0 and virtual worlds to guide the next technological transition and ensure an open, secure, trustworthy,

1 European Commission. (2023). *EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition* (COM(2023) 442 final). https://ec.europa.eu/newsroom/dae/redirection/document/97337

fair and inclusive digital environment for EU citizens, businesses and public administrations.

The new strategy aims to create Web 4.0 and virtual worlds that reflect EU values and principles, where people's rights are fully applied and European businesses can flourish. The strategy is in line with the goals of the Digital Decade policy program for 2030 and its three key areas of digitalisation: skills, business and public services. The fourth strand, infrastructure, is addressed in the Commission's connectivity package and its broader efforts in computing, cloud and edge power.

However, it is fundamentally significant from a legal and philosophical point of view that *the Metaverse is a concept qualitatively broader than Web 4.0* and cannot be reduced to the latter as a technological category. The Metaverse embraces *Web 4.0* as its technological substructure, but goes far beyond it, constituting a fundamentally new socio-legal reality with the following dimensions that are not covered by purely technological characteristics:

Firstly, new social relations and identity: in the Metaverse, full-fledged social interactions emerge between individuals whose digital avatars acquire legal subjectivity; communities based on digital presence rather than physical localisation are formed; new forms of work, creativity, property, and culture are emerging. The Metaverse and closer integration between the physical and virtual worlds will inevitably affect the way we live and work together, generating both a wide range of potential risks and opportunities (European Commission, 2023b)[1].

Secondly, digital legislation as a regulatory response: the technological architecture of Web 4.0 is only a condition for the possibility of the Metaverse, while its full-fledged constitution as a social phenomenon requires the development of a fundamentally new array of legal norms — from the regulation of digital identity and cybercrime to the protection of human rights in an immersive environment. That is why, as the analytical literature for the EU Strategy rightly notes, the Metaverse "cannot exist 'outside the law' — on the contrary, it must evolve along with regulatory mechanisms, interoperability standards, and digital identity."

Thirdly, digital jurisdiction: the Metaverse raises a fundamentally new question of *who* and *how* exercises power in a cross-border, decentralised, technologically mediated space. This dimension is not covered by any purely technical characteristic of Web 4.0 — it is a phenomenon of the legal and public administration. Sharing (legal relations regarding the sharing, exchange or provision of temporary access to resources, property, services or data, which are governed by the norms of civil, information, digital and sometimes administrative law) global standards for open and interoperable virtual worlds and Web 4.0 is carried out with the aim of ensuring that they are not under the control of several large players (Taylor Wessing, 2023)[2]. However, this task in the systemic dimension concerns the Metaverse — as a jurisdictional exercise environment, and not only the Web 4.0 technical protocol.

---

1 European Commission. (2023, July 11*). An EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition*. https://digital-strategy.ec.europa.eu/en/library/eu-initiative-virtual-worlds-head-start-next-technological-transition

2 Taylor Wessing. (2023, September 4). *EU strategy for leadership in Web 4.0 and virtual worlds.* https://www.taylorwessing.com/en/insights-and-events/insights/2023/09/the-eus-strategy-to-lead-on-web-4

Thus, the conceptual architecture can be reflected in the following hierarchy: *Metaverse = Web 4.0 + new social relations + digital legislation + digital jurisdiction*. Web 4.0 is the technological core of the Metaverse, its necessary but not sufficient condition. The Metaverse is a full-fledged civilisational phenomenon that constitutes a new legal reality, which needs to be comprehended not only from technological, but also from philosophical, legal, sociological and regulatory positions.

The European Commission's communication of July 11, 2023 defines Web 4.0 as a watershed technological transition to a world where everything is seamlessly interconnected. At the same time, the European Council called on the EU to remain at the forefront of Web 4.0 development back in March 2023, and virtual worlds — that is, components of the Metaverse — are seen as an important part of this transition.

It is significant that even in the European Commission's own terminological evolution, it de facto captures this conceptual difference: the Commission in its Communication has deliberately abandoned the term "Metaverse" in favour of "virtual worlds", thereby emphasising the technology-neutral and value-oriented nature of regulation (Bird & Bird, 2023).[1] This suggests that the EU's regulatory logic *does not equate* Metaverse with a technology standard, understanding it in a broader — socio-legal — sense.

Thus, the topic "Metaverse and Web 4.0: from the latest technologies to a new philosophy and legal reality" is methodologically correctly formulated: it reflects the logic of ascent from the partial (technological) to the general (legal philosophy), from the means (Web 4.0) to reality (Metaverse), from the instrumental (digital protocols) to the normative (digital law and jurisdiction). In our opinion, the main heuristic potential of this study lies in this movement — from the technological revolution to the legal one.

The expansion of platform governance practices and "private" moderation/authorisation procedures (which de facto perform regulatory functions) has created a demand for research on minimum standards of due process in digital spaces, as well as on the concept of legal interoperability — i.e. the ability of rules, evidence, and decisions to be "transferred" between different platforms and jurisdictions without losing legal force.

At the same time, the available studies are mostly situational in nature: they focus on individual elements of digital reality (personal data, content moderation, smart contracts, intermediary liability, electronic evidence, AI risks, local ODR models), but do not offer a holistic institutional and regulatory solution for the case where the digital ecosystem functions as a multi-entity environment with internal rules, its own mechanisms of digital self-governance and transnational effects. In view of the above, the scientific problem lies not so much in the lack of individual developments as in the lack of integration of these lines into a single legal model suitable for comprehensive settlement.

It follows that the topic of a comprehensive solution of the outlined challenges through the formation of digital jurisdiction as a regulatory and procedural regime, the development of a digital code as a systematised tool of legal regulation, as well as through

1 Bird & Bird. (2023, July 14). *European Commission presents EU vision for Web 4.0 and virtual worlds.* https://www.twobirds.com/en/insights/2023/global/european-commission-presents-eu-vision-on-web-40-and-virtual-worlds

the conceptualisation of the philosophy of digital ecosystems as a single social, legal and technological mechanism — in the doctrine in a holistic form, has not previously been the subject of consistent and systematic consideration. Based on the analysis, this gap and requires integration into a single theoretical and legal mechanism "architecture - modes - trust - jurisdiction", which determines the relevance of the dissertation research aimed at an institutional combination of existing approaches to the legal ontology of the Metaverse and the removal of tools from it that ensure legal interoperability, accountability, due process and legal protection in cross-border digital ecosystems.

1.1.1. Terminology.

The term Metaverse (Metaverse**)** comes from multiverse or meta-universe and consists of two term elements "meta", which means "without limits, infinity", and "universe". The concept of Metaverse means a hypothetical set of all possible real-life parallel universes, including the one in which we are.

The definitions of the Metaverse are still ambiguous. This creates many variations that are used in popular literature and widely used when describing events taking place in virtual realities (Dzoban, 2021).[1] The Metaverse and the digital human are filled with a variety of information about real-world events and the human prototype from different sources of information (Kostenko, 2020)[2].

Today, this term acquires in the full sense of "cross-border meaning", since an electronic virtual space is created that functions continuously. In the Metaverse, physical entities, through their reflections in digital entities - avatars, interact with each other and electronic objects using information and communication technologies.

The term *Metaverse* entered public intellectual circulation thanks to Neal Stephenson, who in 1992 described a stable, socially saturated virtual space with the presence of users through avatars in the novel Snow Crash. At the same time, the etymological interpretations of "Metaverse" as a derivative of *meta-* ("beyond", "above", "after") and *universe* ("Universe") in scientific texts are more explanatory than normative: in law and regulatory documents, the key is not the origin of the word, but the functional model of the environment — that is, *what kind of social relations* arise, *what technological modules provide them*, and *by what means the state/platform/community carries out regulation and coercion*.

In the technohistorical dimension, the origins of the Metaverse are often associated with early VR research: experimental display and immersion systems that laid the foundation for modern XR practices (VR/AR/MR). The scientific tradition mentions, in particular, the prototypes of helmets/displays of the 1960s (I. Sutherland's line of research) and the development of the first VR virtual reality system known as the "Sword of Damocles" (Eve, 2018; Emerson, 1993)[3, 4] in the concept of the "Last Display"

1 Dzioban, O. P. (2021). *Entsyklopediia sotsiohumanitarnoi informolohii*. Helvetica Publishing House

2 Kostenko, O. V. (2020). Identification data management: Legal regulation and classification. *Scientific Journal of Polonia University*, *43*(6), 198–204. https://doi.org/10.23856/4325

3 Eve, S. (2018). Augmented reality. In *The Encyclopedia of Archaeological Sciences*. https://doi.org/10.1002/9781119188230.saseas0054

4 Emerson, T. (1993). Mastering the art of VR: On becoming the HIT Lab cybrarian. *The Electronic Library, 11*, 385–391. https://doi.org/10.1108/EB045261

(Billinghurst, 2021; Garassini & Mattei, 1994),[1] [2]which allowed users to interact with a virtual environment (Sra & Pattanaik, 2023; Rosenblum, 2000)[3,4].

In the 1980s, American scientist Jaron Lanier developed the first commercial VR system (Carvalho et al., 2022; Mishra, 2016)[5,6].

In the 1990s, the concept of the Metaverse began to develop in the field of computer games, in particular, in the game "Ultima Online" (Willis, 1997)[7], which allowed players to interact with each other in the virtual world. In the 2000s, the concept of the Metaverse began to develop in the field of social networks, in particular, in the "Second Life" network (Willis, 2007)[8], which allowed users to create their own virtual avatars and interact with other users in the virtual world. In the 2010s, the concept of the Metaverse began to develop in the field of virtual and augmented reality, in particular, with the advent of VR/AR technologies.

Further, the concept of a "live" virtual world evolved into massively networked environments (MMOs) and social platforms, where the avatar became a tool for social interaction, economic transactions, and cultural identity. This trajectory is important for law: the Metaverse grows not as a "game" or as a "chat", but as a space of quasi-real activity, in which acts have legal consequences (property, tort, fraud, discrimination, personal data, jurisdictional collisions).

At the present stage, it is advisable to define the Metaverse as a converged digital environment that integrates immersive interfaces (XR), network infrastructures, identity (avatars/profiles), algorithmic modules (AI/agents), as well as economic and social institutions (virtual assets, smart contracts, community rules, moderation). Within the framework of the study, a basic definition is proposed: "Metaverse is an electronic environment formed by a set of electronic subjects and objects that interact with each other, as well as technologies that ensure their interaction" (Figure 1). Legal consequences directly branch off from this definition:

1) the emergence *of electronic subjects* (avatars, digital personalities, autonomous agents),
2) the emergence *of electronic objects* (smart assets, tokens, virtual real estate, digital twins),
3) the need for *electronic jurisdiction* as a special regime of regulation and protection of rights.

---

1 Billinghurst, M. (2021). Grand challenges for augmented reality. *Frontiers in Virtual Reality, 2*, 578080. https://doi.org/10.3389/frvir.2021.578080.

2 Garassini, S., & Mattei, M. (1994). Evening presentation: The state of the art in virtual reality. (pp. 385–388). https://doi.org/10.1007/978-1-4899-1004-2_25

3 Sra, M., & Pattanaik, S. (2023). Enhancing the sense of presence in virtual reality. *IEEE Computer Graphics and Applications, 43*, 90–96. https://doi.org/10.1109/MCG.2023.3252182

4 Rosenblum, L. (2000). Virtual and augmented reality 2020. *IEEE Computer Graphics and Applications, 20*, 38–39. https://doi.org/10.1109/38.814551

5 Carvalho, B., Soares, M., Neves, A., Soares, G., & Lins, A. (2022). The state of the art in virtual reality applied to digital games: A literature review. In *Advances in Ergonomics in Design, Usability and Special Populations: Part I*. https://doi.org/10.54941/ahfe100811

6 Mishra, D. (2016). Virtual reality. In *SpringerReference*. https://doi.org/10.1007/springerreference_7381

7 Day, G. (2001). Online games: Crafting persistent-state worlds. *Computer, 34*, 111–112. https://doi.org/10.1109/2.955104

8 Willis, H. (2007). The unexamined Second Life isn't worth living: Virtual worlds and interactive art. *Afterimage*, *35*(2), 13–16. https://doi.org/10.1525/AFT.2007.35.2.13.

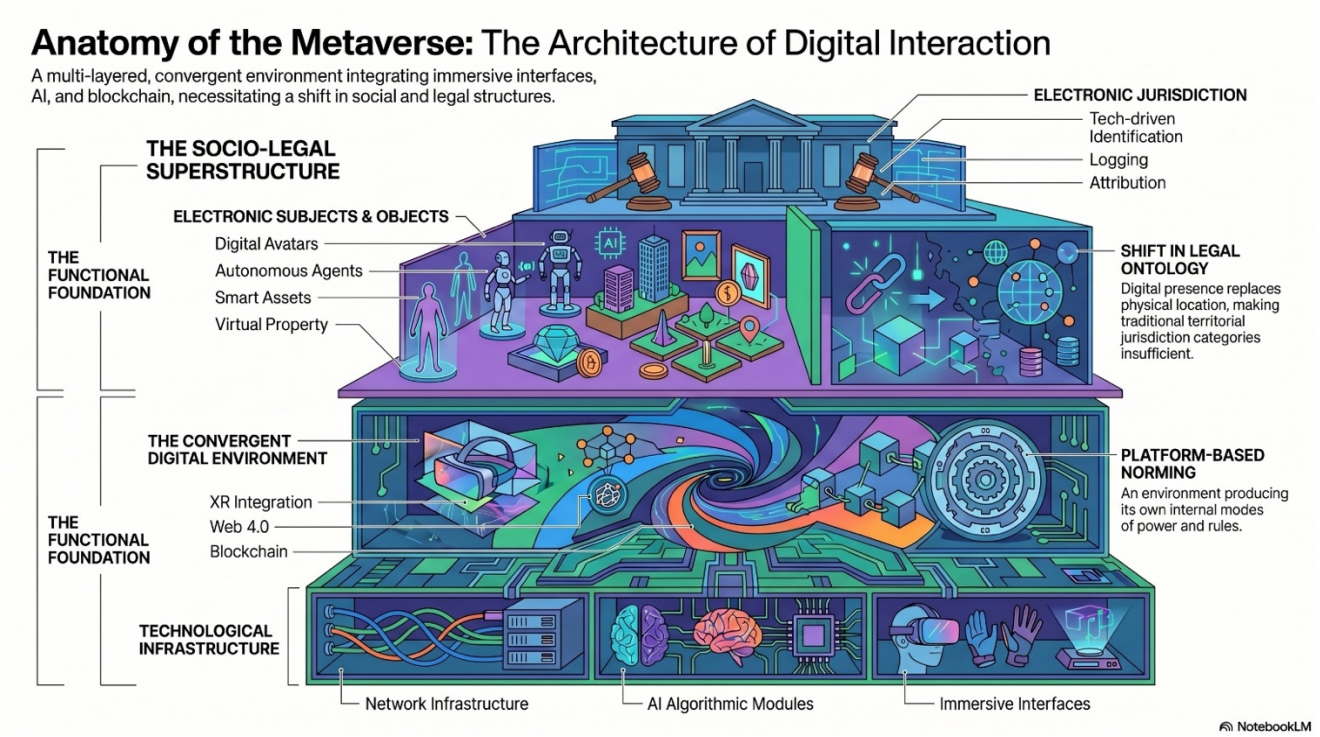


Figure 1. What is Metaverse.

The Metaverse, in contrast to classical information systems, forms a new ontology of social existence, in which "presence" acquires a digital mode, and legal personification is increasingly mediated by digital identity. This raises a fundamental legal problem: traditional categories of *territory*, *competence*, *jurisdiction* and *localisation of legal relations* do not "disappear", but become insufficient without technological binding mechanisms (identification, logging, attribution of actions, evidence of data, interoperable standards). In this sense, the Metaverse should be interpreted not as an "extension of the Internet", but as an environment that produces its own regimes of power and regulation — this is an analytical position that needs to be further expanded in sections on the nature of "platform rules" and their relationship with public law.

At the current stage of development of digital civilisation, the Metaverse appears as a convergent environment that combines elements of virtual, augmented and mixed reality, as well as social, economic, legal and cultural interactions in the virtual space. In the future, the term Metaverse will be understood as a multidimensional digital space in which immersion technologies, Web 4.0, blockchain, digital avatars, artificial intelligence (AI) virtual ecosystems, virtual identities and smart assets interact in real time, creating conditions for a new form of legal relations – the legal space of virtual systems, or *"Metaverse is an electronic environment formed by a set of electronic subjects and objects that interact with each other, as well as electronic or other technologies that ensure their interaction"* (Kostenko, 2022a)[1].

1 Kostenko, O. V. (2022). Problemy pravovoho rehuliuvannia metavsesvitu [Problems of legal regulation of the metaverse]. In *Modern science: Innovations and prospects: Proceedings of the V International Scientific and Practical Conference* (pp. 729–734). https://www.researchgate.net/publication/359209336_Problems_of_legal_regulation_of_the_metawerse_problemi_pravovogo_reguluvanna_metavsesvitu

The Metaverse phenomenon, unlike classical information systems, is not only a technical innovation – it embodies a new ontology of social existence, where physical presence is replaced by digital presence, and a legal entity acquires quasi-physical personification through digital identity. In this context, the deployment of the Metaverse requires a rethinking of the philosophical foundations of law, in particular the categories of legal personality, jurisdiction, nature of property, identity, and spatio-temporal localisation of legal relations (European Parliamentary Research Service, 2022) (European Parliamentary Research Service, 2022)[1]. In general, the Metaverse is not a continuation of classical cyberspaces, but is formed as an autonomous ontological reality that produces its own models of interaction, ethics, power structures, and legal regimes. It is in this environment that there is a need to form a digital jurisdiction adapted to the non-hierarchical, decentralised, and transnational nature of virtual spaces (Allam & Allam, 2024)[2].

The methodological foundations for the formation of the conceptual apparatus are based on the fact that definitions in the field of digital law perform not a reference function, but a qualification function: they must be suitable for identifying legally significant facts, determining the subject composition, establishing regimes of rights and obligations and further application in resolving controversial and problematic issues of legal regulation. In this case, the basic one is the combination of the doctrinal (dogmatic) method with systematic, functional and comparative legal approaches, which allows you to reconcile the technical and economic descriptions of the Metaverse with the categories of legal regulation (data mode, digital identity, transactions, responsibility). Based on the analysis, the technique of conceptual engineering was applied: each key concept is introduced together with a regulatory core, a minimum set of legal features and test criteria for application.

To ensure internal consistency of terminology, an ontological approach is also used, which in the legal dimension means the construction of a legal ontology of the Metaverse as a system of interrelated concepts about subjects, objects, events and procedures of normative importance. The practical value of this approach lies in the fact that it supports legal interoperability (consistency of categories between different modes of governance and jurisdictions) and reduces the risk of "splitting" definitions between technical and legal discourses. In view of the above, the concepts in the subsection are structured as elements of a future ontological model suitable for further formalised description of digital jurisdiction (Oliveira et al., 2024)[3].

Today, the definition of Metaverse is formed taking into account the interdisciplinary heterogeneity of scientific discourse: modern reviews and systematisations describe the Metaverse as a convergence of virtual worlds, XR interfaces, network infrastructures, digital asset economies, and algorithmic agents that provide a long-term "presence" and interaction in real time. Hence the methodological rule: each technical token (XR, blockchain, AI, digital twins) in the conceptual apparatus is interpreted through legal criteria (identifiability of participants, access control, legal regime of data and content, evidence of actions, accountability). It is this "translation" procedure that makes

1 European Parliamentary Research Service. (2022). *Metaverse: Opportunities, risks and policy implications*. European Union. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733551/EPRS_BRI(2022)733551_EN.pdf

2 Allam, Z., & Allam, Z. (2024). Introduction to the metaverse. In Z. Allam & Z. Allam (Eds.), *The metaverse and smart cities* (pp. 1–18). Elsevier. https://doi.org/10.1016/B978-0-443-22351-8.00013-1

3 Oliveira, V., Zatti, S., Scherer, R., & Nicola, N. (2024). Legal interoperability ontology for international data spaces (LegIOn-IDS). *CEUR Workshop Proceedings*, *3882*, Paper 5. https://ceur-ws.org/Vol-3882/paper5.pdf

definitions suitable for further sub-items on platform evolution and trust as a normative standard (Ning et al., 2021; Wang et al., 2023)[1, 2].

A separate methodological guideline is the European Digital Policy Framework for Web 4.0 and Virtual Worlds, which emphasises the need to combine innovative development with security, trust, and protection of fundamental rights. This means the need to correlate definitions with regulatory requirements (privacy-by-design, security by default, platform accountability, consumer protection) so that the conceptual apparatus immediately "works" as a tool of legal regulation and does not require further regulation conceptual "repair". In view of the above, the comparative dimension in this case is considered as a method of methodological validation: if the definition does not allow for the correlation of the Metaverse phenomenon with standards of trust and accountability, it needs to be clarified (European Commission, 2023a)[3].

The categories of "algorithmic transparency" and "algorithmic accountability" are introduced not as ethical slogans, but as elements of the legal construction of trust: they define the minimum requirements for explainability, auditability, procedural fairness (due process), and distribution of responsibility in the case of automated decisions in the Metaverse. Methodologically, this relies, firstly, on the results of a systematic review of the literature on algorithmic responsibility, which captures the key components of accountability (actors, mechanisms for demanding explanations, control tools and sanctions), and, secondly, on modern conceptual models of governance algorithms that clarify the ratio of transparency, responsibility and legitimation. Based on the analysis, these approaches make it possible to bring algorithmic transparency to the level of a legal standard relevant to digital jurisdiction (Wieringa, 2020; Horneber & Laumer, 2023)[4 5].

The categories of "algorithmic transparency" and "algorithmic accountability" are introduced not as ethical slogans, but as elements of the legal construction of trust: they define the minimum requirements for explainability, auditability, procedural fairness (due process), and distribution of responsibility in the case of automated decisions in the Metaverse. Methodologically, this relies, firstly, on the results of a systematic review of the literature on algorithmic responsibility, which captures the key components of accountability (actors, mechanisms for demanding explanations, control tools and sanctions), and, secondly, on modern conceptual models of governance algorithms that clarify the ratio of transparency, responsibility and legitimation. Based on the analysis, these approaches make it possible to bring algorithmic transparency to the level of a legal standard relevant to digital jurisdiction (Wieringa, 2020; Horneber & Laumer, 2023)[6 7].

---

ing, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2021). *A survey on metaverse: The state-of-the-art, technologies, applications, and challenges*. arXiv. https://doi.org/10.48550/arXiv.2111.09674

2Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, *25*(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

3European Commission. (2023, July 20). *An EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition* (Communication COM(2023) 442 final). https://data.consilium.europa.eu/doc/document/ST-12080-2023-INIT/en/pdf

4Wieringa, M. (2020). What to account for when accounting for algorithms: A systematic literature review on algorithmic accountability. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20)* (pp. 1–18). New York, NY: ACM. https://doi.org/10.1145/3351095.3372833

5 Horneber, D., & Laumer, S. (2023). Algorithmic accountability. *Business & Information Systems Engineering, 65*(6), 723–730. https://doi.org/10.1007/s12599-023-00817-8

6Wieringa, M. (2020). What to account for when accounting for algorithms: A systematic literature review on algorithmic accountability. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20)* (pp. 1–18). New York, NY: ACM. https://doi.org/10.1145/3351095.3372833

7 Horneber, D., & Laumer, S. (2023). Algorithmic accountability. *Business & Information Systems Engineering, 65*(6), 723–730. https://doi.org/10.1007/s12599-023-00817-8

1.1.2. Differentiation of the Metaverse from related categories and working definition.

The separation of Metaverse from related concepts (XR as a technological immersion channel, "virtual worlds" as separate digital environments, cyberspace as a broader information environment, and Web3 as an infrastructure layer of decentralisation) has not only terminological but also directly legal significance. It is through the correct delineation of the boundaries of the concept that the subject of legal regulation, the range of subjects of obligations and the limits of application of the regimes are determined: personal data protection, protection of intellectual property rights, financial monitoring and consumer rights. In this sense, scientific research in the field of the Metaverse proposes to interpret it as a persistent network of interoperable, partially interoperable virtual environments, where social interaction and economic circulation are supported by data, computing and digital identifiers (Wang et al., 2023; Almoqbel et al., 2022; Mystakidis, 2022)[1, 2, 3].

Let's fix the minimum set of criteria in the presence of which the environment can qualify as Metaverse in a legally relevant sense: persistence (continuity of existence and reproducibility of states); multisubjectivity and synchronous interaction; the presence of digital identity and representation mechanisms (avatar/profile/keys); infrastructure of legal "binding" of digital assets (virtual assets, tokenised objects, access rights); procedural rules of governance and moderation that affect the rights and obligations of participants; cross-border and interoperability (at least at the level of data exchange protocols).

These criteria correlate with the regulatory vision of the United States, China, and the EU, which see virtual worlds as the next technological transformation that requires a combination of innovation policies with legal safeguards and accountability (European Commission, 2023a; Ning et al., 2021)[4, 5].

Based on the above, the author's definition of the Metaverse within the framework of this study is formulated as: Metaverse *is a multi-level immersive digital environment of interaction between electronic subjects and objects, in which persistent virtual spaces, digital identity, data, content and virtual assets are combined by access protocols, algorithmic governance and circulation rules that create legally significant legal relations.*

In view of the above, such a definition sets the boundaries of further analysis of the subject composition, objects of rights and normative mechanisms of digital jurisdiction.

Subjects, Objects, and Legal Roles in the Metaverse

In the subject dimension of the Metaverse, the key is the notion of digital identity as a legally relevant ability to be recognised in the environment and to link actions in virtual space with responsibilities, rights, and protection procedures. At the technical and legal

1 Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *arXiv.* https://arxiv.org/abs/2203.02662.

2 Almoqbel, M. Y., Naderi, A., Wohn, D. Y., & Goyal, N. (2022). The metaverse: A systematic literature review to map scholarly definitions. *CSCW '22 Companion.* https://doi.org/10.1145/3500868.3559448

3 Mystakidis, S. (2022). Metaverse. *Encyclopedia, 2*(1). https://doi.org/10.3390/encyclopedia2010031

4 European Commission. (2023, July 11). *Web 4.0 and virtual worlds: A head start in the next technological transition* (Communication COM(2023) 442 final). https://digital-strategy.ec.europa.eu/en/library/web-40-and-virtual-worlds-head-start-next-technological-transition

5 Ning, H., Wang, H., Lin, Y., et al. (2021). A survey on metaverse: The state-of-the-art, technologies, applications, and challenges. *arXiv.* https://arxiv.org/abs/2111.09673

level, this implies distinguishing between identification (identification), authentication (confirmation of control over the means of access) and attribution of the action (assigning an event to the subject). Application of decentralised identifiers (DIDs) and frameworks European Digital Identity allows for the construction of more interoperable models of evidentiary suitability, while at the same time raising the question of the appropriate level of guarantees of privacy and procedural fairness (W3C, 2022; European Parliament & Council, 2024a)[1] [2].

The concept of "avatar" in the legal ontology of the Metaverse should be interpreted as a digital representative of the subject that functions as an interface for participation in legal relations (communication, concluding agreements, creating content, moving in space, participating in the "rules of the environment"). That is why the avatar cannot be considered solely as a visual image: in a number of scenarios, it plays the role of a procedural "bearer" of rights and obligations, including the preservation of evidence, compliance with moderation rules and fulfilment of obligations. Based on the analysis, it can be assumed that the formation of separate guarantees for the protection of digital identity (protection against account theft, avatar spoofing, fraud with digital assets) should become an element of Metaverse regulation and a component of digital jurisdiction (European Parliament & Council, 2024a)[3].

Separately, it is necessary to distinguish the "digital twin" as a digital model (representation) of a physical object or process from an avatar as a representation of a person. A digital twin in the Metaverse, in particular in industrial scenarios, can be an object of intellectual property rights, the subject of access and use agreements, as well as a source of data for management decision-making and recommendations. In view of the above, the systematisation of doctrinal approaches to digital twins in the technical sciences is expedient to the extent that it allows for the legally correct construction of modes of access, responsibility and evidence (Jones et al., 2020; da Silva Mendonca et al., 2022; NIST, 2025)[4, 5, 6].

1.1.3. Metaverse Objects: Typology and Legally Relevant Attributes.

In the Metaverse, the object scope of legal relations covers at least four classes:
1) data (personal, behavioural, biometric, spatial),
2) content (audiovisual, textual, programmatic, generative),
3) digital items (virtual items, access rights, licences, inventory) and
4) virtual assets as objects of economic circulation.

For legal ontology, it is important to record that in one "life cycle" of interaction of a Metaverse participant, these classes often merge: a digital object is simultaneously

---

1 World Wide Web Consortium (W3C). (2022). *Decentralized identifiers (DIDs) v1.0 — Core architecture, data model, and representations.* W3C Recommendation. https://www.w3.org/TR/did-core/

2 European Parliament & Council of the European Union. (2024, April 11). *Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS).* https://eur-lex.europa.eu/eli/reg/2024/1183/oj

3 European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union (OJ L).* https://eur-lex.europa.eu/eli/reg/2024/1183/oj

4 Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology, 29*, 36–52. https://doi.org/10.1016/j.cirpj.2020.02.002

5 da Silva Mendonça, R., et al. (2022). Digital twin applications: A survey of recent advances and challenges. *Processes, 10*(4), 744. https://doi.org/10.3390/pr10040744

6 National Institute of Standards and Technology (NIST). (2025). *Digital identity guidelines (NIST Special Publication 800-63-4).* https://doi.org/10.6028/NIST.SP.800-63-4

content, data, and a carrier of value, which creates collisions between the regimes of data protection, intellectual property, and property rights (Verkhovna Rada of Ukraine, 2022)[1].

It is advisable to use the concept of "virtual assets" as a legal category that allows describing tokenised objects, rights of claim, digital units of value, and other forms of property rights that arise in digital environments. The European Approach (MiCA) introduces a classification of crypto assets and establishes requirements for issuers and service providers, which is relevant for Metaverse economies, where the circulation of tokens is integrated into the logic of access, management, and settlements. Ukrainian legislation on virtual assets, in turn, is important for determining the terminological framework and limits of the lawful circulation of such objects in the national legal order (Rada of Ukraine, 2022)[2,3].

A specific type of digital objects in the Metaverse is NFTs, which technically certify the uniqueness of the record (token), but are not identical to the intellectual property right to a digital work or model. This necessitates a clear contractual construction: what rights are transferred together with the token, what licence conditions apply, who is responsible for copyright infringement, and how the protection of a bona fide acquirer is ensured. Based on the analysis of doctrinal positions, it is suggested that Metaverse environments require standardised "legal package" designs (licence + access terms + resale mode) that provide legal interoperability between platforms (Ochoa, 2024; Girsang, 2024)[4, 5,]. In view of the above, the distinction between "token" and "rights" should be a cross-cutting principle of further regulatory analysis (FATF, 2021; European Parliament, 2022)[6, 7].

1.2. Metaverse as an object of legal regulation: structural and functional characteristics, life cycle and interaction

The Metaverse as a sociotechnical environment functions not only through "rules of use", but also through algorithmic mechanisms that affect access, content visibility, moderation, ratings, resource allocation, and even "behavioural corridors" of participants. In this regard, it is advisable to understand the categories of "algorithmic transparency" and "algorithmic accountability" as legal tools for reducing risks and legitimising decisions made in an automated or semi-automated manner. Algorithmic auditing and the concept of transparency in the public sector offer holistic approaches to capturing metrics,

1 Verkhovna Rada of Ukraine. (2022, February 17). *Law of Ukraine "On virtual assets" №. 2074-IX*. Vidomosti Verkhovnoi Rady Ukrainy. https://zakon.rada.gov.ua/laws/show/2074-20

2 European Parliament & Council of the European Union. (2023, May 31). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA).* https://eur-lex.europa.eu/eli/reg/2023/1114/oj

3 Verkhovna Rada of Ukraine. (2022, February 17). Law of Ukraine "On virtual assets"№. 2074-IX. Vidomosti Verkhovnoi Rady Ukrainy. https://zakon.rada.gov.ua/laws/show/2074-20

4 Ochoa, T. T. (2024). Non-fungible tokens and copyright law. *Santa Clara High Technology Law Journal, 40*(4). Retrieved from https://digitalcommons.law.scu.edu/chtlj/vol40/iss4/3

5 Girsang, W. (2024). Legal issues about NFTs and related technologies. *Academic Journal of Interdisciplinary Studies.* https://doi.org/10.36941/ajis-2024-0073

6 Financial Action Task Force (FATF). (2021, October). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

7 European Parliament. (2022). *Intellectual property rights and distributed ledger technology (DLT).* https://www.europarl.europa.eu/RegData/etudes/STUD/2022/737709/IPOL_STU(2022)737709_EN.pdf

verification procedures, and documenting solutions that can be adapted to Metaverse environments (Kossow, 2021; National Institute of Standards and Technology, 2023)[1, 2].

The regulatory frameworks emerging at the international and European levels emphasise the need for a risk-based approach, lifecycle management of AI systems, and ensuring human control. In particular, the NIST AI RMF proposes a risk management framework, while the EU AI Act establishes requirements for transparency, data management, documentation, and oversight for defined categories of systems. Additionally, UNESCO's ethical standards emphasise the principles of non-discrimination, respect for human rights and responsibility. In view of the above, the integration of these frameworks into Metaverse regulation can be accomplished through standards for moderation, access, explainability, and appeal mechanisms (National Institute of Standards and Technology [NIST], 2023; European Parliament & Council of the European Union, 2024; NIST, 2023; (UNESCO, 2021)[3, 4, 5, 6].

In a legal context, this has a direct impact on digital jurisdiction: algorithmically driven decisions (blocking an account, removing content, restricting access to virtual assets) require minimum due process standards, including notification, motivation, the ability to view and preserve evidence. Thus, algorithmic transparency in the Metaverse is not only a "technical" requirement, but a component of the legal assurance of trust and accountability, which will be expanded in the following sections (FATF, 2021; European Parliament, 2022a)[7, 8].

1.2.1. Features of the Metaverse as an object of normalisation.

On the basis of the formed conceptual and categorical apparatus, it is proposed to single out the legal features of the Metaverse as an object of regulation: persistence and reproducibility of the digital environment; protocol of access and interaction, which gives rise to "rules of the environment"; the presence of digital identity and action attribution mechanisms; economic turnover of virtual assets integrated into the functioning of the environment; algorithmic governance and moderation as a source of legally significant decisions; multi-level trust (technical, organisational, procedural) as a condition for legitimacy; cross-border and multiplicity of potential jurisdictions; the evidentiary nature of data and event logs, which requires standards of conservation and admissibility.

---

1 Raji, I. D., Scheuerman, M. K., Zearfoss, S., et al. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *arXiv.* https://arxiv.org/abs/2001.00973

2 Kossow, N. (2021). *Algorithmic transparency in the public sector.* https://law-ai.org/wp-content/uploads/2021/03/Kossow-Algorithmic-Transparency.pdf

3 National Institute of Standards and Technology (NIST). (2023). *Artificial intelligence risk management framework (AI RMF 1.0).* https://www.nist.gov/itl/ai-risk-management-framework

4 European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://eur-lex.europa.eu/eli/reg/2024/1689/oj

5 UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000380455

6 National Institute of Standards and Technology (NIST). (2023, January). *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1).* https://doi.org/10.6028/NIST.AI.100-1

7 Raji, I. D., Scheuerman, M. K., & Zearfoss, S. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAccT '20).* (pp. 33–44). https://doi.org/10.1145/3351095.3372873

8 Kossow, N., Windwehr, S., & Jenkins, M. (2021). *Algorithmic transparency & accountability: Safeguards in the use of algorithmic systems.* Transparency International. https://www.transparency.org/en/publications/algorithmic-transparency-accountability-safeguards-in-the-use-of-algorithmic-systems

In view of the above, it is this set of features that distinguishes the Metaverse from separate "virtual worlds" and justifies the need for separate mechanisms of digital jurisdiction (European Parliament & Council, 2023a)[1].

The proposed features perform two functions: firstly, they provide a methodological discipline for further analysis, cutting off excessive technicality and philosophising, which does not give rise to legal consequences; secondly, they allow the construction of normative regimes relevant to the life cycle of legal relations in the Metaverse (identification-access-interaction-transaction-dispute-coercion/recovery). Based on the analysis, it can be assumed that such a "matrix of features" will become a supporting structure for the study (Anidjar et al., 2023)[2].

1.2.2. Phases of development of Metaverse platforms and the evolution of regulatory regulation of digital ecosystems.

Within the framework of the study, the "Metaverse platform" is understood as an organisational and technical infrastructure in which the rules for access, moderation and circulation of digital objects are established, the mechanisms of digital identity and attribution of actions are implemented, and transactionality (economic, communicative, evidence-based) is ensured. Scientific reviews of the development of the Metaverse as a multi-technological socio-economic system confirm that the key "nodes" of evolution are related not only to XR or networks, but to models governance, security, and privacy (Sun et al., 2022)[3]. In view of the above, further phases of development are outlined through a change in the source of rules and legal regimes, and not through marketing characteristics or brand names.

1.2.3. Methodology for periodisation of Metaverse platforms.

It is proposed to establish phases according to a set of four criteria:

1) the subject of control and the source of rule-making (terms of use and policies of the platform; "Community law"; public regulation; protocol/DAO governance);

2) the regime of digital objects and virtual assets (licensed access and revocable rights vs tokenised circulation and/or legal protection of individualised digital things);

3) a model of digital identity and attribution of actions (centralised registration; federated schemes; decentralised identifiers and verifiable statements);

4) institutional contour of dispute enforcement (internal moderation; alternative dispute resolution; state jurisdiction; electronic jurisdiction as a special regime).

This approach makes it possible to tie technological shifts to legal facts and legal consequences.

Platform-Centric Phase: Immersive Worlds as a "Platform Jurisdiction".

Early and mature corporate platforms are characterised by the dominance of private regulation: the rules of conduct, content, sanctions, and appeal procedures are formed by the operator as part of the Agreement of Accession (Terms of Service).

---

1 European Parliament & Council of the European Union. (2023, May 31). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA).* https://eur-lex.europa.eu/eli/reg/2023/1114/oj

2 Anidjar, L. Y., Packin, N. G., & Panezi, A. (2023). The matrix of privacy: Data infrastructure in the AI-powered metaverse. *Harvard Law & Policy Review, 18.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4363208

3 Sun, J., et al. (2022). Metaverse: Survey, applications, security, and opportunities. *arXiv.* https://arxiv.org/abs/2210.07990

The legal consequence is the transformation of a significant part of legal relations into the plane of "private governance", where the following become central:

a) transparency and fairness of contractual terms;

b) due process in moderation and blocking;

c) the accountability of the platform as an intermediary/intermediary regarding content and security risks.

In EU law, this logic is clearly supported by an approach that establishes graduated duties for intermediary services depending on their function and size, as well as by regimes of competitive neutralisation of the "gates" of digital markets (European Parliament & Council, 2022a)[1]. Based on the analysis carried out, it is advisable to emphasise: in this phase, the main object of legal assessment is not the "virtual world" as such, but the power of the platform over the rules, data and access.

Tokenised phase: partial property participation and compliance reality.

The next stage is characterised by the emergence of a managed economy of digital things: the circulation of tokenised objects, internal markets, the use of smart contracts, the combination of social interaction with financial incentives. Legally, this means that along with licence structures, there are user's property expectations that require legal qualification (right of claim/right of access/right to dispose of a digital asset), as well as the importance of compliance (AML/CFT risks, consumer protection, conflicts of interest of marketplaces). In European law, the vector of regulation of virtual assets and services with them is reflected in a special regulation on markets in crypto-assets (European Parliament & Council, 2023b)[2].

Therefore, we directly deduce "virtual assets" as a bridge between the platform economy and the future digital ownership block, and also indicate how tokenisation changes the approach to proof (transaction chain, auditability, trace preservation).

Protocol phase: interoperability, mutual recognition, ecosystems.

The protocol (interoperable) phase of Metaverse development marks a qualitative change in the regulatory architecture: the dominance of the "closed" platform as a single centre of rule-making is gradually giving way to the model of a network of environments, within which the user expects portability of his digital identity, property rights to virtual assets, and legally acquired content between different worlds (Figure 2).

The legal meaning of this transition is that "platform law" (ToS) can no longer remain the only source of certainty: there is a demand for supra-platform interoperability rules that function as protocol standards — technical and at the same time normatively relevant.

1 European Parliament & Council of the European Union. (2022, September 14). *Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act).* https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

2 European Parliament & Council of the European Union. (2023, May 31). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA*). OJ L 150, 9.6.2023, p. 40–205. https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

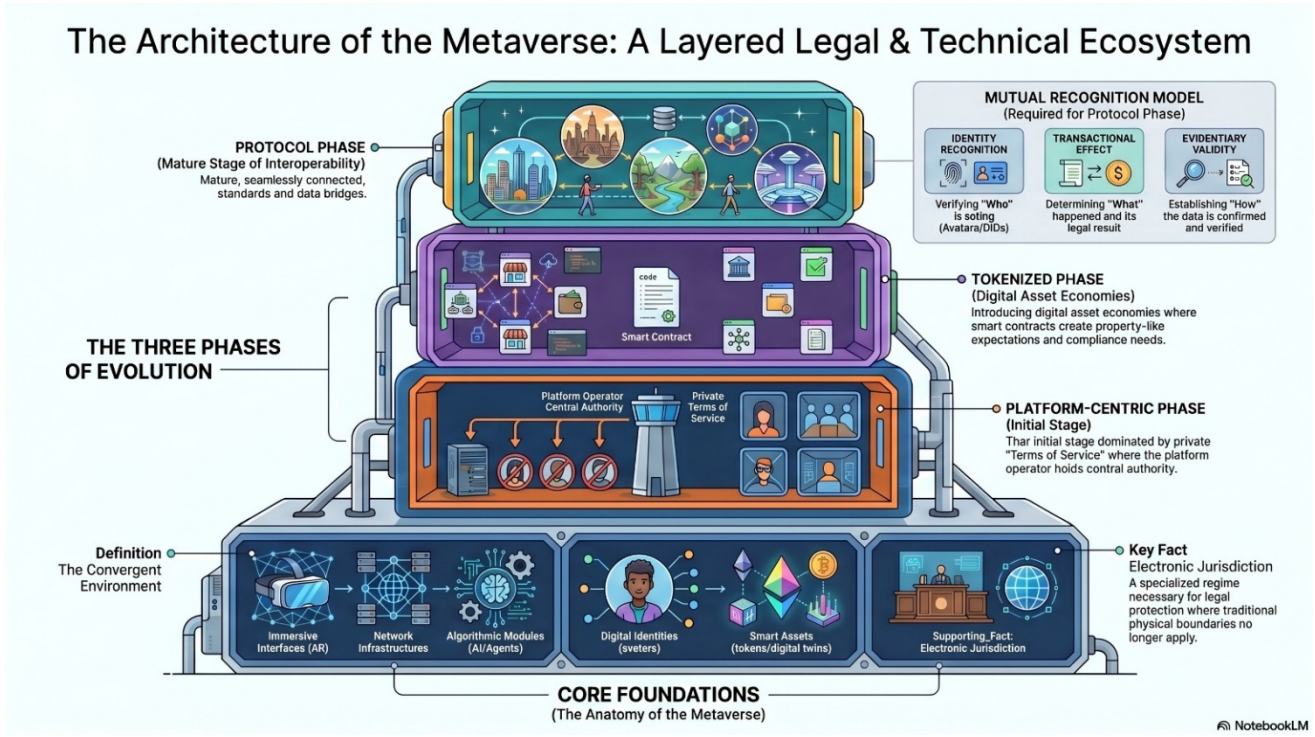


Figure 2. The Metaverse Evolution Cycle.

Within this phase, interoperability should be understood not as a purely engineering compatibility of data formats, but as legal interoperability, i.e. the ability of different environments to recognise the legal consequences of actions carried out in another environment. That is why protocols (as well as standards and specifications) acquire a quasi-jurisdictional meaning: they set the "framework" of permissible transactions, attribution of actions, and the evidentiary suitability of events. This logic fits into the concept of "protocol jurisdiction" as a regime determined not by the territory, but by the standard/protocol of network functioning, taking into account interoperability and security rules (ISO, W3C, TCP/IP, blockchain protocols are mentioned, in particular). That is, the protocol becomes a "bridge" between the technical nature of the Metaverse and the legal ontology of legal relations within it.

The basic problem of the protocol phase is the mutual recognition of legal facts: whether one provider recognises the identity, transaction or legitimacy of an asset created in a different environment. Thus, "mutual recognition" in the Metaverse should be conceptualised as a comprehensive mode that spans at least three levels:

1) recognition of identification data (who acts);

2) recognition of transactions and their consequences (what exactly happened and with what legal effect);

3) acknowledgment of evidence (as it can be confirmed and verified).

Such a three-layer model makes it possible to separate the portability of the "account" from the portability of "rights", and the portability of "rights" from the portability of "evidentiary traces".

In this part, it is advisable to tie the national legal context of Ukraine to the regulatory framework of electronic identification and electronic trust services, since it creates legal mechanisms for attribution of actions and recognition of electronic evidence/signatures in the digital environment. The Law of Ukraine "On Electronic Identification and

Electronic Trust Services" directly defines the legal and organisational principles for the provision of electronic trust services, including cross-border ones, which is methodologically consistent with the idea of mutual recognition in multi-entity digital ecosystems (Verkhovna Rada of Ukraine, 2017; Verkhovna Rada of Ukraine, 2010)[1,2]. Therefore, in the dissertation, it is logical to emphasise: the interoperability of the Metaverse requires not only API interoperability, but also a "trust" infrastructure capable of ensuring the legal stability of identification, authentication and integrity of electronic actions.

At the same time, the protocol phase exacerbates the issue of the legal regime of virtual assets in the context of their transfer between platforms. It is important for Ukraine to fix the regulatory vector, but correctly indicate its current status: the Law of Ukraine "On Virtual Assets" No. 2074-IX is marked in the legislative base as not having entered into force, with a specially defined mechanism for entering into force. That is why it is appropriate to talk in the text about the "regulatory waiting mode" and compliance practices of providers, without replacing this with a statement about the complete completion of the legislative architecture. At the same time, it is impossible to ignore the Law of Ukraine "On Personal Data Protection" as a basic regime for identity/data portability and minimising the risks of profiling in cross-platform transfers.

The European regulatory logic is indicative here: the Digital Markets Act (Regulation (EU) 2022/1925) aims to ensure "controversial and fair" digital markets and establishes obligations for gatekeepers, which is directly aligned with the aim of neutralising the lock-in effect and stimulating interoperability in large ecosystems. This allows us to formalise the thesis: interoperability in the Metaverse is not only a technical characteristic, but also a subject of competitive and legal balance between innovation and market openness.

Equally important is the EU's policy and regulatory signal on the transition to Web 4.0 and virtual worlds, and relevant EU initiatives explicitly focus on openness, security, trust, and interoperability as a condition for the next technological transition (Fernandez et al., 2022). This [3]is consistent with the official position of the European Commission in the Web 4.0/Virtual Worlds Strategy, which emphasises the intention to form global standards for open and interoperable virtual environments and not to allow them to be dominated by "a few big players". That is, it is interoperability that becomes the "trust" for the formation of digital jurisdiction as a regime of mutual recognition, evidence-based governance, and procedural legitimacy

1.2.4.Web 1.0-3.0 as a prerequisite for the Metaverse.

The genesis of Metaverse platforms demonstrates the movement from gaming and social prototypes to corporate/industrial environments (digital twins, collaborative design, learning simulators, remote presence). In a legal sense, this means a change in the "risk profile": while early environments dominantly generated disputes over content and

1 Verkhovna Rada of Ukraine. (2010, June 1). *Law of Ukraine "On personal data protection" №. 2297-VI*. Vidomosti Verkhovnoi Rady Ukrainy, (34), Article 481. https://zakon.rada.gov.ua/laws/show/2297-17/ed20221027#Text

2 Verkhovna Rada of Ukraine. (2017, October 5). *Law of Ukraine "On electronic trust services"* №. 2155-VIII. Vidomosti Verkhovnoi Rady Ukrainy, (45), Article 400. https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005#Text

3 Fernandez, C. B., et al. (2022). Life, the metaverse and everything. *arXiv.* https://arxiv.org/abs/2204.01480

behaviour, modern environments dominated disputes over data, biometrics, authorship, virtual assets, fraud, labour relations in VR work, security, and discrimination. The pandemic period accelerated the legitimation of remote presence, but it did not create the Metaverse itself: it only increased the social demand for the "presence effect" that video conferencing does not provide.

The beginning of the Metaverse can be considered the development of interactive computer games such as Super Mario. The entertainment industry offered the user control of an electronic avatar, which performs certain tasks in electronic decorations and uses game electronic attributes. The growth of digital power has changed interactive games and brought their perception closer to the real elements of the physical world, since video conferencing, video communication, video broadcasting have exhausted themselves precisely because they cannot fully provide the effect of presence and interpersonal visual-verbal and tactile communication with traditional social roles.

Most Metaverse platforms, like digital currencies, are powered by blockchain technology. We can predict that the next significant leap in the development of electronic reality may occur soon and this will be due to the end of the processes of "extraction" of the last of the 21 million. bitcoins. The finalisation of bitcoin "mining" will release countless powerful video cards and computing modules, which will be refocused on ensuring the functioning of electronic avatars. In addition, the functioning of the Metaverse requires the exchange of super big data, which will stimulate the widespread adoption of 5G and 6G technologies, cloud services, and software development.

The following can be attributed to the well-known Metaverse platforms.

Microsoft Mesh is the "enterprise Metaverse" in Microsoft's Azure cloud. Users can interact with each other using virtual avatars, and, at the same time, are physically located in different places. You can connect to the Metaverse using a VR headset, smartphone, personal computer, and the HoloLens-2 AR headset from Microsoft. In the future, the introduction of "holoportation" processes (from the word "hologram") in a virtual office, in order to conduct working communication and meetings. Nvidia Corp is similar in concept to Microsoft.

The plan is to create a public workspace between avatar architects to co-model Metaverse objects and subjects. Epic Games is developing its own Metaverse of the same name, Epic Games, which will be dedicated to interactive fantasy games. Facebook is considering launching different Metaverse platforms at the same time, from electronic cities such as Santa Monica to educational platforms (GigaCloud, n.d.)[1].

Korean companies LG Display Co., Ltd. and Samsung are working towards creating an electronic Metaverse city "Seoul" on the Seoul Metaverse platform, which users can access using the FlickPlay app. So far, the functionality is limited to the ability to make excursions and individual purchases.

Chinese search giant Baidu has launched a project to colonise the first planet Metaverse Xirang (Land of Hope). The project was developed on the Baidu virtual platform in the form of a giant virtual Möbius ribbon. The project involves the simultaneous functioning of up to 100 thousand avatars participating in the Baidu AI

1 GigaCloud. (n.d.). *What is the metaverse, why does business need it, and why is it built on cloud technologies*. https://gigacloud.ua/blog/navchannja/scho-take-metavsesvit-navischo-vin-biznesu-i-chomu-jogo-budujut-na-hmarnih-tehnologijah

Developer Conference. Other Chinese state-owned telecommunications companies - China Mobile, China Unicom and China Telecom have merged with technology companies Tencent Holdings Ltd, ByteDance and NetEase Inc. to form the Metaverse Industry Committee, China's first industry group, with the aim of mass settlement of the Metaverse by Chinese citizens (ZN. UA, n.d.)[1].

In a general scientific sense, we consider three phases of development, which will be detailed in the following sections of the work:

1) platform-centric phase, where the rules and assets are controlled by the developer;

2) mixed phase, where the user receives partial property and management rights (through tokenisation/smart contracts/market);

3) decentralised/autonomous phase, where the environment is not reduced to a single owner, and governance is distributed between the protocol, community, and agents (including autonomous ones).

Regarding the problem of possible "autonomous" (without human intervention) functioning of the avatar and the Metaverse, it should be noted that there are risks of cases when the autonomous Metaverse can actually become an artificial "extraterrestrial" life form, since then humanity may lose the actual impact on its objects, subjects and development processes.

The legal significance of the developmental phases is important for the further justification of digital jurisdiction (Figure 2). The evolution of Metaverse platforms is a movement from private rule-making (ToS mode) to mixed models of economic participation (virtual assets) and further to protocol interoperability and algorithmic autonomy.

In each phase, the following changes: the source of the rules; the status of subjects and digital identity models; volume and quality of evidentiary traces; mechanisms of coercion and appeal. It is this "legal periodisation" that creates a logical transition to a generalised technological architecture of the Metaverse, and this architecture is considered here not "by itself", but as an infrastructure of legal regimes subject to digital jurisdiction.

1.3. Web 4.0\Metaverse Concept in the European Union: Regulatory Vectors, Standards, and Regulatory Approaches

1.3.1. Web 4.0\Metaverse Concept and European Union

In the European legal tradition, Web 4.0\Metaverse is considered not as a "next-generation gaming space", but as a technological and legal framework for the emergence of new digital relationships: from identity (avatar/digital profile) and property rights (digital assets) to responsibility for the actions of autonomous agents and compliance platforms. The EU has consistently approached the Metaverse as a sociotechnical infrastructure that requires agreed standards (interoperability), security and human rights guarantees, as well as enforcement mechanisms in a non-territorial environment.

In the scientific and legal analysis of the Metaverse, it is advisable to proceed from the fact that its "technical nature" is the primary matrix for further construction of the

1 ZN. UA. (n.d.). *While Gates and Zuckerberg are promising, China is populating the metaverse.* https://zn.ua/ukr/SOCIUM/poki-hejts-i-tsukerberh-obitsjajut-kitaj-zaseljaje-metavsesvit.html

legal ontology of virtual environments, and not just a description of engineering parameters. That is why the technical properties of the Metaverse should be interpreted as *normatively relevant* characteristics: they determine which models of jurisdiction, responsibility, identification, and ownership can be legally stable in the immersion space. The affirmation is consistent with the approach according to which the Metaverse appears not just a "platform", but a convergent environment of a new form of legal relations and a new mode of the subject's presence through digital identity.

According to an analytical briefing by the European Parliamentary Research Service (EPRS), the ideal Metaverse model is described through four technical features: realism, ubiquity, interoperability, and scalability. At the same time, realism is associated with the emotional immersion of the user; ubiquity — with the availability of virtual spaces through different digital devices using one virtual identity; interoperability — with the ability of platforms/systems to seamlessly exchange information and interact; scalability — with the ability of the network architecture to support mass participation without compromising the quality of the experience.

In view of the above, these four properties can be considered as "threshold conditions" for the legitimacy of digital identity in the Metaverse. If realism builds trust in the avatar as a quasi-physical representation of a person, then ubiquity *legally pushes* towards a model of a "single (or mutually agreed) digital identity" that preserves the stability of legal personality during migration between services and devices. In this context, digital identity ceases to be a purely technical function account and acquires the features of a legal institution that requires separate guarantees of non-compliance, authenticity and controllability.

No less important is that interoperability and scalability form the basis for the virtual economy: they make possible the turnover and portability of virtual assets, as well as the mass of transactions and interactions. EPRS directly points to the expected reliance of the Metaverse economic ecosystem on blockchain solutions and crypto assets, in particular NFTs, as tools for monetisation and fixation of rights to digital objects (European Parliamentary Research Service, 2022). In Ukrainian legal discourse, this correlates with the thesis that NFTs, smart contracts, and "virtual lands" in environments like Decentraland and The Sandbox function as real electronic intangible assets, with which legally significant actions are carried out.

The dimension of self-government in virtual communities needs special emphasis. The EPRS briefing captures the competition of two visions: "privatised" (corporately managed) and "community" (community form), where communities build and manage their own worlds. In our opinion, at this point, technical "protocol governance" moves into the plane of digital self-government, and therefore requires legal regulation of participation mechanisms, delegation of powers, transparency of rules and procedures for appealing decisions (in particular, moderation decisions, bans, restrictions on access to assets).

However, at the same time as open prospects, the Metaverse actualises a set of risks that have direct regulatory weight. EPRS emphasises the scale of data collection and processing (including biometric and emotional/physiological response data), which reinforces the requirements for legal regimes for personal data protection and cybersecurity, as well as the practical problems of proper user consent and countering the

theft of avatar identity. The expansion of the data plane in the Metaverse effectively means that legal protection should cover not only "personal information" but also *behavioural and bodily-like digital traces* that form a new area of vulnerability.

According to the EPRS briefing "Metaverse: Opportunities, risks and policy implications", there is a problem of legal qualification of digital assets (virtual assets, digital things/quasi-things, content rights, "virtual property"), as well as the issue of legal interoperability, i.e. consistency of legal regimes between different platforms and jurisdictions. Effective legal regulation of relations in the Metaverse inevitably rests on the differences in the regulations of different jurisdictions regarding identification, copyright, ownership of non-property assets, and liability. It is this multiplicity of modes that makes the harmonisation of technical and legal standards not optional, but a system-forming task of regulating the Metaverse.

In view of this, within the legal ontology of the Metaverse, it is fundamentally important to record that the descriptive "technical properties" of the Metaverse are not a neutral engineering reference, but act as determinants of future legal regulation. In other words, the technical architecture sets the framework for which models of responsibility, digital identity, circulation of virtual assets and digital self-governance mechanisms can be stable and executable in the virtual environment.

According to the European Parliamentary Research Service (EPRS) briefing "Metaverse: Opportunities, risks and policy implications, 2022", the Metaverse in an ideal model has four basic technical characteristics: realism, ubiquity, interoperability, and scalability are directly "translated" into the plane of law as prerequisites for the formation of digital identity and its legal verification regimes. If ubiquity in the technical sense implies a single identity for different devices and environments, then in the legal dimension it pushes towards the requirement of legal interoperability of identification solutions (consistency of attributes, proof of authenticity, procedural restoration of access, counteraction to person/avatar substitution). In our opinion, this is where the need arises to distinguish a platform account from a legal institution of digital identity, for which there should be guarantees of the subject's control over their own identification data.

Further, interoperability and scalability form the foundation of the virtual economy, as they enable mass transactions and the portability/portability of digital objects between environments. EPRS highlights that the Metaverse economic ecosystem is expected to rely on blockchain solutions and crypto assets, particularly NFTs, to monetise transactions in the digital environment, while immediately actualising the issues of ownership, abuse, interoperability, and portability of such assets. In the legal plane, this means the inevitability of doctrinal and normative qualification of virtual assets (as objects of civil circulation, as holders of property rights, as digital evidence), as well as the development of minimum standards of traceability, bona fide acquisition and mechanisms for protecting rights.

However, at the same time as the open prospects, the Metaverse actualises a complex set of risks in the field of personal data protection and cybersecurity. The EPRS explicitly states that the "huge amount of data" in the Metaverse gives rise to data protection and cybersecurity issues, including issues of user consent and avatar protection from identity theft. Moreover, the briefing highlights the massive collection of sensitive data, including

biometric and data on users' emotional and physiological responses, which requires specific legal safeguards and clearly articulated processing purposes.

In this regard, the issue of harmonisation of technical and legal standards is becoming central — both at the level of interoperability protocols and at the level of cross-border data exchange and asset portability. The Council of Europe, in a separate analytical paper on the impact of the Metaverse on human rights, the rule of law and democracy, emphasises that legal rules, ethical guidelines and technical standards can support transparent data practices, In particular, in cross-border transfer, sharing and portability between applications, and points out the importance of informed consent, cyber protection and user agency. Council of Europe (Council of Europe & IEEE. (n.d.)[1] complementarily, ITU in the Metaverse Standardization Roadmap (FGMV-51, 2024) (ITU,n.d.)[2] directly emphasises the role of international standardisation to ensure interoperability, security, and consistency of approaches, which in the legal dimension reinforces the argument about the need for "legal support of standards" as part of Metaverse regulation (Pereira, 2025).[3]

In the strategic vision of the European Union, the Metaverse is outlined not only as a technological innovation but also as a key tool for stimulating economic development. According to analytical estimates, by 2035, the adoption of Metaverse technologies is expected to provide the EU with gross domestic product growth of between €259 billion and €489 billion, equivalent to 1.3% to 2.4% of the European Union's aggregate GDP. Such a scale of influence determines the urgent need for the introduction of comprehensive legal regulation, with an emphasis on the regulation of digital property issues, the protection of personal data and the prevention of violation of the principles of fair competition in the virtual environment.

Industrial applications of Metaverse technologies have already been implemented in certain sectors of the economy. For example, BMW and TotalEnergies use digital twins to increase operational efficiency, optimise production processes, and reduce costs. These digital models make it possible to predict technical failures, ensure the adaptability of production systems to changes in market conditions, and reduce equipment downtime by a third[4].

The EU sees the Metaverse as a new paradigm of social and legal relations emerging in deeply immersive virtual environments, where classic boundaries between online and offline environments are blurred. Digital identity, avatar status, intellectual property in digital form, as well as guarantees of user rights in virtual spaces have become key issues of global interdisciplinary discussion (European Commission, 2023)[5]. The transformation

1 Council of Europe & IEEE. (n.d.). *The metaverse and its impact on human rights, the rule of law and democracy.* https://rm.coe.int/the-metaverse-and-its-impact-on-human-rights-the-rule-of-law-and-democ/1680b178b0

2 International Telecommunication Union (ITU). (n.d.). *FG-MV deliverables.* https://www.itu.int/en/ITU-T/focusgroups/mv/Documents/List%20of%20FG-MV%20deliverables/FGMV-51.pdf

3 Pereira, A. (2025, February 20). *Legal challenges in the metaverse.* Record of Law. https://recordoflaw.in/legal-challenges-in-the-metaverse/

4 Meta. (2023, May). *The metaverse and the opportunity for the European Union.* https://www.mondodigitale.org/sites/default/files/allegati/pagina/2024/The%20Metaverse%20and%20the%20Opportunity%20for%20the%20EU.pdf

5 European Commission. (2023, July 11). *Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds.* https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718

of the nature of legal personality in the context of the Metaverse demonstrates the need to rethink the foundations of the traditional legal order.

One of the most controversial aspects is the legal qualification of avatars, digital entities, electronic personalities and their behaviour in the virtual environment. The question arises: can the digital projection of a person acquire the characteristics of a traditional subject of law, or will it remain only its virtual representative or a formal "mirror"? The report of the European Parliamentary Research Service emphasises the importance of shaping new approaches to responsibility in the Metaverse space, in particular in relation to digital property, interaction with autonomous agents and AI assistants (European Parliamentary Research Service, 2022)[2]. Practice already records cases of theft or unauthorised duplication of digital assets, which causes significant difficulties in establishing a responsible party and an effective redress mechanism.

One of the key challenges facing law in the context of the development of metaverses is the formation of an effective legal mechanism for regulating digital property rights, in particular in the field of virtual asset circulation. The Metaverse creates conditions for transactions with digital objects, including NFTs, virtual real estate, tokenised assets, which are often subject to fraudulent schemes due to a lack of legal certainty and the difficulty of identifying violators in a distributed digital environment (European Commission, 2023). While the use of blockchain technologies partially improves the transparency of transactions, it does not solve the fundamental question: how should national and international law be applied in extraterritorial virtual jurisdictions?

The problem of cybersecurity in VR/AR environments is no less acute. Practice shows that digital crimes — from unauthorised access to avatars and digital assets to hacking personal profiles — are becoming commonplace in metaverses. There are known cases of theft of digital items and manipulation of users' biometric data due to vulnerabilities in XR platforms. Therefore, the task of introducing preventive and reactive legal protection mechanisms is urgent, in particular, the institutionalisation of digital courts as structures authorised to consider offences within the digital jurisdiction of the Metaverse.

In 2024, the convergence of law, artificial intelligence, and the Metaverse will witness a number of transformational changes. These changes are shaped by key developments in both the global and European legal systems, changing the future of these rapidly evolving digital spheres.

1.3.2. The regulatory trajectory of the Metaverse in the EU strategy.

The formation of a consistent "normative trajectory" for the regulation of meta-environments: from the unification of approaches to intellectual property to competition law, the protection of industrial designs, and ethical restrictions on the use of artificial intelligence is a logical necessity of the modern digital environment. Such a legal "telescopic spyglass" makes it possible to see the reference points at which the Metaverse is no longer perceived as a purely technological experiment, and increasingly as an infrastructural sphere of digital markets where a new legal ontology of digital objects

(digital works, virtual assets, designs, models of behavioural interaction and tools for influencing the user's will) is being formed (European Parliament, 2024a)[1].

The first reference point is the joint position of the heads of patent and trade offices of the G7 countries on the protection of intellectual property rights in "new digital contexts", in particular in the Metaverse (the discussion took place on December 15, 2023 in the "Metaverse format"). It is indicative in that it does not record the creation of a "parallel" regime, but the confirmation of the applicability of the current intellectual property rules to virtual circulation, with an emphasis on law enforcement and countering violations (piracy, counterfeiting, trademark abuse) in digital spaces. Thus, the Metaverse in G7 logic is outlined as an environment where continuity of legal protection should operate, and not an "exclusive zone" without a right (G7 Heads of IP Office Conversation, 2023)[2].

The second line of the regulatory shift is the European Commission's initiatives in the field of competition law: in January 2024, separate calls for submission of positions on competition in virtual worlds and generative AI were launched. It is conceptually important that the Commission directly links virtual worlds with the risks of structural market concentration (network effects, tipping, barriers to entry, integration of value chains), i.e. it shifts the discussion from the level of futurology to the level of instrumental antimonopoly diagnostics. This means: legal interoperability and technical openness (standards, protocols, data portability, non-discriminatory access) are becoming not only engineering slogans, but also potential criteria for assessing market power (European Commission, 2024a)[3].

The third element is the position of the European Parliament, which, in its resolution of January 17, 2024, insists that policies on virtual worlds must be aligned with EU values and fundamental rights, and that a "clear, comprehensive regulatory framework" becomes decisive as soon as the technology reaches maturity. The text of the resolution particularly clearly articulates the risks to data protection, competition, consumer rights, cybersecurity and intellectual property, as well as a warning against the manipulative design of digital services (European Parliament, 2024a). This creates a normative "framework" in which digital identity, avatar, virtual assets, and behavioural data cease to be "derivatives" of a game or platform, but require autonomous legal regulation.

The fourth benchmark is the modernisation of the design protection regime in the EU: the interim agreement of the Council of the EU and the European Parliament of December 5, 2023 on the "designs package" is aimed at updating almost twenty years of regulation for the challenges of the digital environment and 3D printing, as well as procedural simplification and harmonisation. For the Metaverse, this is of practical importance, since virtual worlds produce arrays of "visual solutions" (interface elements, digital objects, avatar aesthetics, visual markers of brands), which in real circulation

1 European Parliament. (2024, January 17). *European Parliament resolution of 17 January 2024 on virtual worlds – opportunities, risks and policy implications for the single market (2022/2198(INI)) (P9_TA(2024)0032)*. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0032_EN.html

2 G7 Heads of IP Office Conversation. (2023, December 15). *Joint statement.* Ministry of Economy, Trade and Industry / Japan Patent Office. https://www.meti.go.jp/english/press/2023/pdf/20231218001-1eng.pdf

3 European Commission. (2024, January). *Competition in virtual worlds and generative AI: Calls for contributions.* Directorate-General for Competition. https://competition-policy.ec.europa.eu/system/files/2024-01/20240109_call-for-contributions_virtual-worlds_and_generative-AI.pdf

require a fast and effective mode of protection against copying and unfair reproduction. In other words, the design in the Metaverse acquires the characteristics of an economic asset, which directly affects the configuration of the virtual economy (Council of the European Union, 2023)[1].

The fifth — and, in our opinion, the most methodologically acute — is the line of ethical and security restrictions on AI in Metaverse environments. On January 22, 2024, unofficial consolidated texts on the future of the EU AI Act were circulated in the public space, which allowed the expert community to see the "ban architecture" and implementation mechanics (in particular, the timing of the application of individual blocks). At the same time, it is the final regulation on AI in the EU that enshrines the ban on practices, related to subliminal techniques or exploitation of vulnerabilities of individuals/groups, when this can significantly distort behaviour and cause significant harm; for the Metaverse, this is directly relevant, because immersivity enhances the effect of influencing the user's will (IAPP, 2024)[2].

In view of the above, the above documents build a single regulatory plot (Figure 3):

1) IP protection and enforcement in "new digital contexts";

2) competition policy as a safeguard against platform monopolisation of virtual worlds and generative AI;

3) human rights, data protection and prevention of manipulation as a normative "threshold of what is acceptable";

4) updating the design as a regime of legal protection of digital forms;

5) AI-compliance as a tool for controlling the risks of behavioural influence.

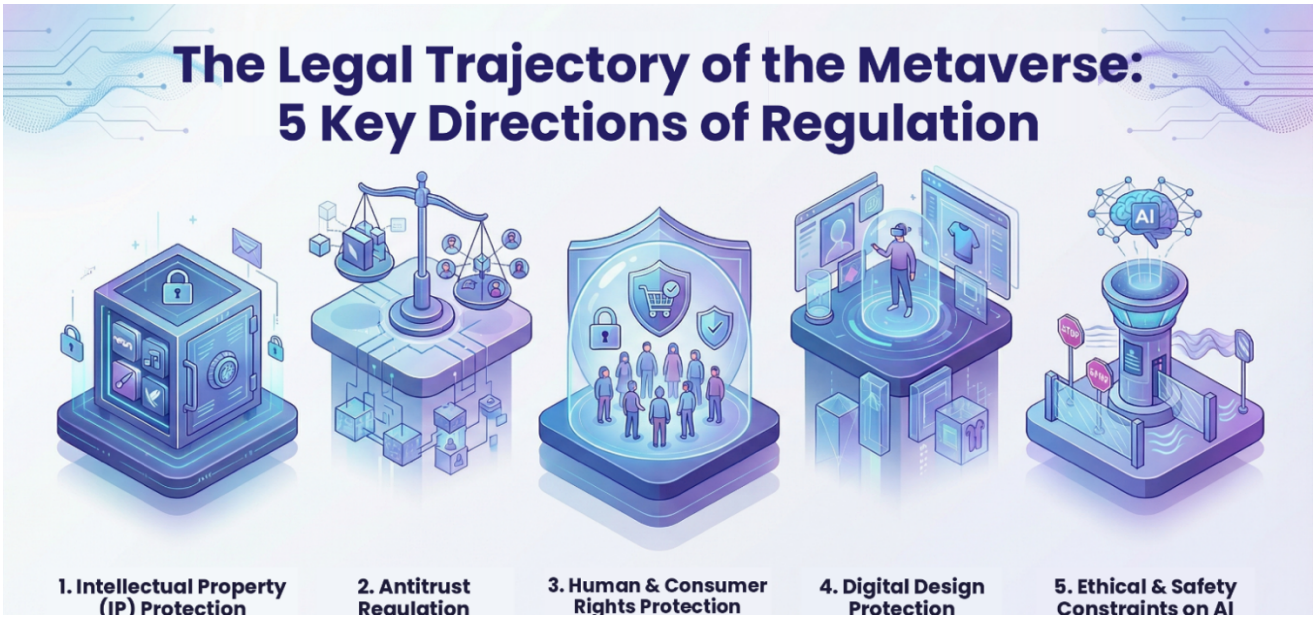


Figure 3. Metaverse: legal trajectory.

1 Council of the European Union. (2023, December 5). *Council and Parliament strike provisional deal on design protection package* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2023/12/05/council-and-parliament-strike-provisional-deal-on-design-protection-package/

2 International Association of Privacy Professionals (IAPP). (2024, January 22). *EU AI Act: Draft consolidated text leaked online.* https://iapp.org/news/a/eu-ai-act-draft-consolidated-text-leaked-online/

Taken together, this forms the basis for digital self-governance in virtual communities not as "platform self-regulation", but as a legally meaningful order, where platform rules must be interoperable with law (in the sense of compatibility of procedures, standards of evidence, protection of rights and liabilities) (Taylor Wessing, 2024a; Taylor Wessing, 2024b)[1, 2].

1.3.3. EU Web 4.0\ Metaverse Strategy.

Web 4.0 Strategy and "Virtual Worlds": The European Trajectory of Digital Jurisdiction. The European Commission conceptualises the transition to Web 4.0 and virtual worlds as a political and legal process where technical development should be subordinated to the principles of security, openness, accountability and human rights. In this approach, the Metaverse cannot exist "outside the law" — on the contrary, it must evolve along with regulatory mechanisms, interoperability standards, and digital identity; This is where the idea of digital jurisdiction as a set of norms, institutions and procedures for dispute resolution and liability in virtual systems is "embedded".

EU regulatory "props" relevant to the Metaverse: Data Act as a data and access regime. For the Metaverse, not only the "right to content" becomes decisive, but also the right to data generated by devices and environments (XR/IoT/digital twins). In this sense, the Data Act is important because it sets out the rules for fair access to and use of data (including B2B/B2C access models, data transfer to third parties, etc.). For research logic, this means: a Metaverse digital jurisdiction will inevitably have a "data-centric" component — mechanisms for access, portability, control, and responsibility for data processing in distributed ecosystems. According to official European materials, the Data Act entered into force on 11.01.2024 and began to apply on 12.09.2025.

AI Act as a "risk framework" for Metaverse AI agents and trust in autonomous systems. For the Metaverse, where content, moderation, personalisation, recommendations, simulations, and even "avatar behaviour" are increasingly generated or driven by AI, the EU AI Regulation (AI Act) is becoming key. Its systemic role is not to "describe AI", but to establish a risk-based architecture of responsibilities (bans, requirements for high-risk systems, transparency, supervision, compliance), which will directly affect the design and operation of Metaverse platforms. Official EU documents state that the AI Act entered into force on 01.08.2024; separate obligations for general-purpose models (GPAI) are introduced in stages — and this is critical for the Metaverse, because GPAI models are often the "core" of intelligent agents and content generation.

In response to these challenges, the European Commission has initiated the development of a Web 4.0 Strategy covering integrated Metaverse regulation within the framework of EU social, economic and digital policies. The main priorities are to ensure safe, fair and inclusive access of citizens to the digital environment, develop unified standards for digital identity, protect users' rights to digital assets, as well as adapt existing legal systems to the conditions for the functioning of virtual reality. Thus, the concept of

1 Taylor Wessing. (2024, January). *Evolving legal paradigms in AI and the metaverse.* https://www.taylorwessing.com/en/insights-and-events/insights/2024/01/evolving-legal-paradigms-in-ai-and-the-metaverse

2 Taylor Wessing. (2024, January). *The interfaces between artificial intelligence and the Data Act.* https://www.taylorwessing.com/en/insights-and-events/insights/2024/01/the-interfaces-between-artificial-intelligence-and-the-data-act

digital jurisdiction, based on a combination of technological solutions and legal norms, is becoming a promising tool for digital justice.

In particular, the European Commission's strategy paper emphasises the need to develop uniform interoperability standards for metaverses, which will ensure the free exchange of digital assets between platforms and reduce the risk of creating centralised ecosystems controlled by large corporations (European Parliament, 2023)[1]. It is also planned to introduce digital inclusion mechanisms that will allow people with disabilities or low levels of digital literacy to use Metaverse services on equal terms.

In addition, the Web 4.0 strategy envisages the creation of regulatory sandboxes to test new digital technologies under controlled conditions before their full-scale implementation. This will allow the EU to develop a flexible yet effective system of legal control over digital environments, ensuring a balance between innovation and the protection of users' rights (Meta, 2023; European Parliamentary Research Service, 2022; European Commission, 2024b)[2, 3, 4].

1.3.4. USA and Metaverse.

The American model, unlike the European one, tends towards sectoral and precedent-setting "imposition" of the right to new digital practices: constitutional guarantees of freedom of expression, federalism, a strong role of terms of service and self-regulation. This means that in the US, "Metaverse law" is not being formed as a codified act, but as a legal mosaic of privacy, consumer protection, financial compliance, copyright, and criminal law prohibitions that adapt to VR/AR/XR contexts.

For Ukraine, this approach is valuable as proof that, for example, digital jurisdiction can start not from a "perfect code", but from a manageable set of legal regimes, if they are agreed upon by common principles and technical standards of trust. This is confirmed by valuable experience in the formation of legislation in the field of electronic signatures.

Thus, at an early stage, the United States moved precisely along the path of local experiments of states: in the 1990s, various models of "digital signature laws" appeared, often technologically specific (i.e., tied to specific cryptographic approaches or certification infrastructure). Congress directly recorded the problem of incompatibility and "conflicting" approaches of states in materials for the future of E-SIGN, mentioning examples such as states where legal validity was recognised only if a certain technology was used In [5]1999, the Uniform Electronic Transactions Act (UETA) was proposed as a "unified" tool designed to remove barriers to e-commerce by recognising the legal validity of electronic records and electronic signatures in transactions, subject to the

1 European Parliament. (2023, December). *A Europe fit for the digital age: Non-legislative initiative on virtual worlds, such as metaverses.* Legislative Train Schedule. https://www.europarl.europa.eu/legislative-train/carriage/metaverse/report

2 Meta. (2023). *The metaverse and the opportunity for the European Union.* https://www.mondodigitale.org/sites/default/files/allegati/pagina/2024/The%20Metaverse%20and%20the%20Opportunity%20for%20the%20EU.pdf

3 European Parliamentary Research Service. (2022). *Virtual worlds and the metaverse: Opportunities, risks and policy implications.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf

4 European Commission. (2024, May). *Virtual worlds: Trends report.* European Blockchain Observatory and Forum. https://blockchain-observatory.ec.europa.eu/document/download/eccf0cf2-4fc8-469c-8e6b-91fe61d77e74_en?filename=May_2024_Virtual_Worlds_Trends_Report_Final.pdf

5 U.S. Congress. (2000). *Electronic Signatures in Global and National Commerce Act* (H. Rept. 106–341). https://www.congress.gov/committee-report/106th-congress/house-report/341/

consent of the parties to act electronically (NCC USL, 1999) [1]. It should be noted that it was the UETA that in a practical sense served as a "normative template" for states and, thus, accumulated local law-making approaches into a more predictable structure (NCCUSL, 1999; U.S. Congress, 2000). After the "maturation of the problem" in the domestic state space, federal institutionalisation took place: in 2000, Congress passed the Electronic Signatures in Global and National Commerce Act (E-SIGN), which enshrined the basic rule of inadmissibility of denying the legal force of an electronic signature or electronic record only through their electronic form (15 U.S.C. § 7001) (United States Code, n.d.a; United States Code, n.d.b).[2]What is important in the legal technique of E-SIGN is that it is addressed to transactions "in between regular or foreign trade", that is, it is immediately focused on national circulation, where the fragmentation of state rules created the largest transaction costs.

The key "connector" to the two-tier was the design of collision prevention and managed state autonomy. E-SIGN provides that state law may modify/supersede federal regulations only under certain conditions (including through the adoption of UETA or alternative procedures that do not impose a specific technology and are compatible with federal logic)—this is enshrined in 15 U.S.C. § 7002. Therefore, the federation does not "cancel" the law of the states, but sets the corridor of unification, while preserving space for local regulatory structures.

The practical result is a two-tier system: for a significant part of transactions affecting interstate/external commerce, the federal E-SIGN minimum works, while in intrastate legal relations, models based on UETA or special acts of states are widely used. A good example of the "non-identity" of a state solution is New York, which uses its own Electronic Signatures and Records Act (ESRA) for e-signatures and e-records within state jurisdiction (New York State Office of Information Technology Services, 2023)[3].

Thus, the United States first allows for regulatory variations (states as laboratories), but when there is a need for national predictability, it forms a federal act that does not eliminate local regimes, but streamlines them through a mechanism of compatibility and limited preemption. As a result, an architecture emerges where innovation is supported by decentralisation, and legal certainty is supported by a federal "framework" for the validity of electronic signatures (Legal Information Institute. (n.d.). *15 U.S.C. § 7002: Exemption to preemption)*.

The United States of America is a state with a unique law-making experience, in which federalism performs not only the constitutional and organisational, but also the methodological function of a "normative testing ground". In other words, the legal regulation of many new social relations, in particular in the field of digital technologies, often begins not with centralised codification, but with local rule-making of states, which

1 National Conference of Commissioners on Uniform State Laws. (1999). *Uniform Electronic Transactions Act (UETA).* https://www.uniformlaws.org/viewdocument/final-act-21?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments

2 United States Code. (n.d.). 15 U.S.C. § 7002 – Exemption to preemption. https://www.govinfo.gov/content/pkg/USCODE-2023-title15/pdf/USCODE-2023-title15-chap96-sec7002.pdf

3 New York State Office of Information Technology Services. (2023, April 6). *Electronic signatures and records act (ESRA): New York State information technology guideline NYS-G04-001.* https://its.ny.gov/system/files/documents/2024/05/nys-g04-001-electronic-signatures-and-records-act-esra.pdf

reflects the territorial, socio-economic, and even mental-cultural characteristics of the respective jurisdictions.

In this sense, state legislatures play the role of primary "laboratories of law", where regulatory models are tested, the first definitions, mechanisms of control and responsibility are formed, and empirical material of law enforcement is accumulated. In view of the above, such a plurality of approaches is not an accidental fragmentation, but acts as an instrument of adaptability: it is through the competition of legal decisions and the different speed of response of states that the system gets the opportunity to "test" the viability of norms in real conditions.

Moving on to the next aspect, it is worth noting that as the "problems mature" — that is, when the technological phenomenon becomes massive, generates typical risks and forms a stable contour of public demand — there is a gradual shift of the regulatory centre to the federal level. At this stage, the state, as a rule, forms a normative legal act on a national scale or strengthens federal supervision through regulatory instruments designed to provide minimum standards of unification and legal certainty.

As a result, a two-tier model of legal regulation characteristic of the United States appears: on the one hand, the preservation of local state regimes that can detail or strengthen the requirements, on the other hand, the establishment of a federal "framework" as a basic standard and a guarantee of the unity of the legal space. This architecture allows for both regulatory flexibility and national predictability for the market, users, and law enforcement.

Based on the analysis, it can be assumed that it is this duality — "state approbation - federal crystallisation" — that is one of the key reasons for the high adaptability of the American legal order to technological changes. At the same time, it inevitably generates a specific price: the period of "maturation" of the problem is accompanied by regulatory mosaicism, conflicting approaches, and increased compliance costs for entities operating in the interstate market.

In our opinion, for a comparative legal study of digital jurisdiction and regulation of the Metaverse, such an American experience has a special heuristic value. It demonstrates that effective legal regulation cannot be a one-time act of codification, but a step-by-step process — from local experiments to federal generalisation, which ultimately forms a multi-level system with various mechanisms of flexibility and unification.

At the same time, we emphasise: the above formula is a generalising model, and not a universal rule for all areas; In specific industries, the ratio of state and federal regulation can vary significantly.

At the same time, it is advisable to use this formula for legal modelling of cross-border digital jurisdiction, for federal legal units are replaced by national digital and traditional jurisdictions, which immediately gives an advantage in the formation of interoperability of a cross-border legal act.

In the doctrinal focus of the legal horizon, which is shared by a significant part of American researchers, the Metaverse is conceptualised as the next phase of the Web3 economy: a stable synchronous space of interaction through avatars, where digital assets acquire the functional role of a "value carrier" and transactions acquire the signs of legally significant transactions within and outside the platform. public law instruments for market and risk supervision (consumer protection, anti-fraud, competition policy). In this

context, the "metaenvironment" is interpreted as a superstructure over existing legal categories rather than as an autonomous object that requires a complete restart of the legal system (Anidjar et al., 2023)[1].

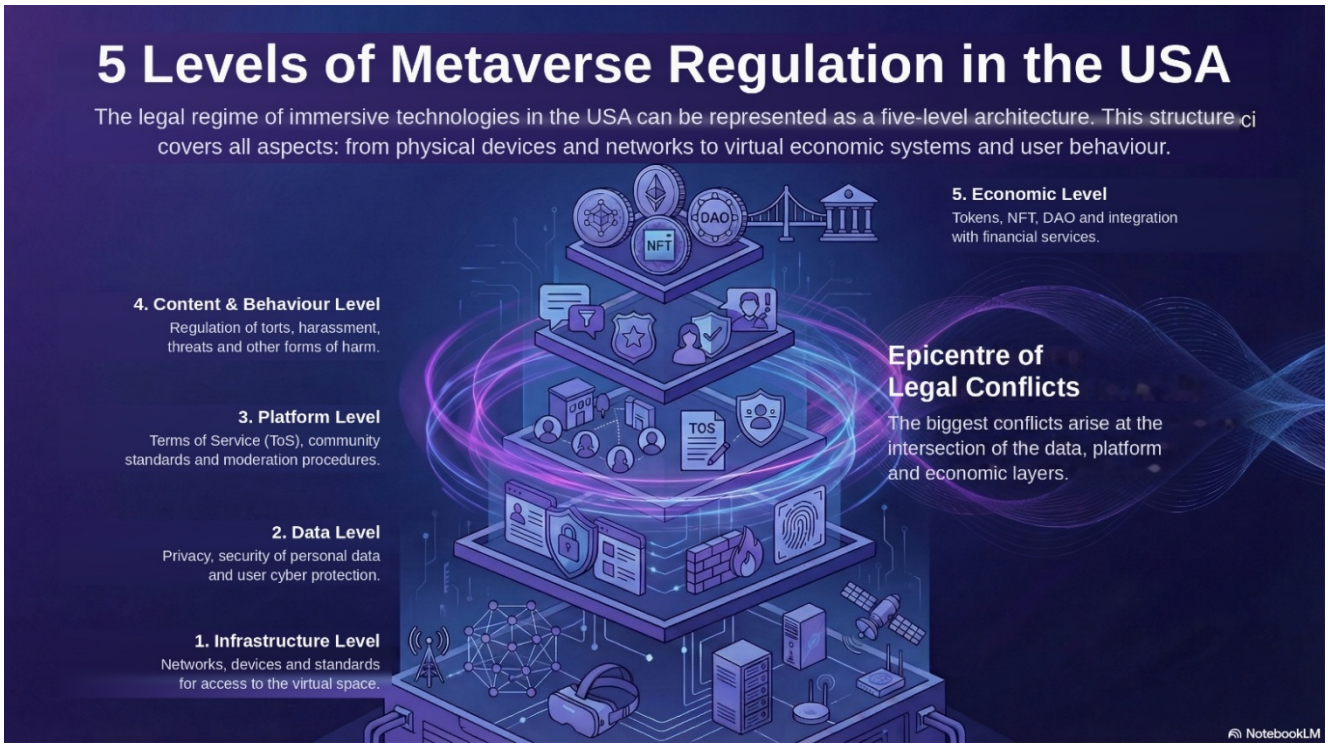


Figure 4. Metaverse: levels of regulation.

Based on the analysis, it is appropriate to describe the legal regime of immersion technologies in the United States as a multi-level architecture (Figure 4):

1) infrastructure level (networks, devices, access standards);

2) data level (privacy, security, cyber protection);

3) the platform level (terms of service, community standards, moderation procedures); Based on the analysis, it is appropriate to describe the legal regime of immersion technologies in the United States as a multi-level architecture (Figure 4):

1) infrastructure level (networks, devices, access standards);

2) data level (privacy, security, cyber protection);

3) platform level (terms of service, community standards, moderation procedures);

4) the level of content and behaviour (torts, harassment, threats, other forms of harm);

5) economic level (tokens, NFTs, DAO elements, integration with financial services).

Practical collisions of the highest density occur where technology simultaneously produces new types of damage and opens up new channels of monetisation, primarily at the levels of data, platforms and the financial ecosystem.

1 Anidjar, L. Y., Packin, N. G., & Panezi, A. (2023). The matrix of privacy: Data infrastructure in the AI-powered metaverse. *Harvard Law & Policy Review, 18.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4363208

At the same time, there is a full-time regulation that makes compliance in the Metaverse legally fragmented. The California CCPA (taking into account further changes related to the CPRA) forms an extensive catalogue of consumer rights and transparency procedures that become practically relevant for platforms working with large amounts of personal data (California Department of Justice, n.d.)[1]The Illinois BIPA is indicative of biometric measurement because it sets out requirements for policies, notifications, consents, and storage/destruction of biometric identifiers, and has historically been associated with high litigation risks (although changes limiting the "plurality" of liability were reported in 2024). In our opinion, it is at this point that the systemic dilemma of the American model manifests itself: the flexibility of innovation is provided by the cost of normative mosaicism and increased unpredictability for the user and the developer.

The financial and regulatory dimension of the "economic Metaverse" tends to the highest density of control when tokenisation, NFT circulation, or DAO practices intersect with traditional financial infrastructure and the risks of money laundering or investment fraud. Such intersections, in view of the above, actually "enable" AML/KYC modes and supervisory mechanisms that do not depend on whether the transaction took place in a physical environment or in a digital simulation. As a result, it is advisable to characterise the American model of Metaverse regulation as decentralised, multi-layered, and fragmented, but at the same time adaptive: it demonstrates that effective regulation can be built not only through a special "meta-law", but also through the consistent adjustment of existing legal regimes. For Ukrainian legal scholars, this creates a valuable contrast: the US demonstrates "regulation as a network of regimes", while the EU demonstrates "regulation as a framework", and it is on this difference that it is convenient to deploy the argument about electronic jurisdiction, legal interoperability, and the design of future digital codes.

1.3.5. PRC and Metaverse.

China and the Metaverse: A State-Centric Model of Digital Environment Management. The Chinese approach (in general terms) is to combine technological expansion with the priority of national security, administrative control, and regulatory discipline of content and platforms. For benchmarking, it is important that such a model is able to quickly create standards and requirements "from the top down", but at the same time generates a different nature of trust: it relies not so much on user autonomy as on the manageability of the ecosystem and the political and administrative accountability of platforms. Here, electronic jurisdiction rather resembles an administrative and legal circuit with a high intensity of control and compliance.

The legal regulation of the Metaverse in the PRC is formed not as a "single law on the Metaverse", but as a state-led configuration of strategic development plans, mandatory cyber and information security requirements, content and data control regimes, as well as private and criminal law norms extrapolated to XR/VR/AR

1 California Department of Justice. (n.d.). *California Consumer Privacy Act (CCPA).* https://oag.ca.gov/privacy/ccpa

environments (Negro, 2025; De Masi et al., 2025)[1,2]. This model organically follows from the Chinese doctrine of "managed digital modernisation": the state simultaneously stimulates innovation and sets "hard boundaries" of what is permissible — primarily where technologies affect political stability, national security, and mass information flows.

In the strategic outline of the PRC, the Metaverse and related technologies (VR/AR, digital twins, AI, next-generation networks) are positioned as the industrial infrastructure of the future and an element of technological competition. Sectoral roadmaps at the level of central authorities are indicative: in particular, official materials of the authorities record that in 2022, relevant ministries/departments published an "action plan" for the integration of VR and industry applications for 2022-2026, where VR is considered as a platform for industry, education, culture, urban government, etc. (Beijing Municipal Government, 2023). [3]This is important methodologically: regulation here "follows the development policy", that is, the state goal and standardisation are determined first, and only then the legal regime of risks is detailed.

The table provides a concise "matrix-like" slice that shows how China is decomposing the Metaverse into regulatory contours (instrumental-legal approach. See Appendices. Table 1).

Control of content and information processes in the "Chinese Metaverse" is not an auxiliary, but a system-forming element. The logic is simple: any XR platform is treated as a kind of Internet information service, and therefore as an object of rules for the dissemination of information, moderation, user identification, and the prevention of "malicious" content. Hence the tendency to form more "isolated" national ecosystems (where external platforms are either displaced or subject to local regulations) and increased technological requirements for providers, including procedural responsibilities for risk management and interaction with regulatory authorities. Unlike the European "regulation-first", the Chinese approach is often "security-first", and the platform's design freedom ends where the management of mass behaviour begins.

The most indicative "legal entry points" in the Metaverse are algorithms and synthetic content. Firstly, the regulator (CAC) deploys tools for administrative supervision of algorithmic services (in particular, through mechanisms for submitting/recording information about algorithms). Secondly, in the field of "deep synthesis", at the level of official clarifications, the need for labelling/identification of synthetic materials and prevention of abuse is emphasised, which is directly relevant to VR environments with avatars, digital copies of voice, face, and behaviour (Cyberspace Administration of China, 2022a)[4]. As a result, the legal risk of the Metaverse in China is

1 Negro, G. (2025). Reading the Chinese metaverse through the past. *European Journal of East Asian Studies.* https://doi.org/10.1163/15700615-02402005

2 De Masi, V., Di, Q., Li, S., & Song, Y. (2025). China's policies and investments in metaverse and AI development: Implications for academic research. *Online Media and Global Communication*, *4*(1), 109–139. https://doi.org/10.1515/omgc-2024-0041

3 Beijing Municipal Government. (2023). *Beijing Internet 3.0 innovation development white paper (2023)* [北京市互联网 3.0 创新发展白皮书]. https://www.beijing.gov.cn/ywdt/gzdt/202305/P020230529616313576667.pdf

4 Cyberspace Administration of China. (2022, December 12). *Zhuanjia jiedu: Guifan shendu hecheng fuwu, yingzao fengqing qizheng de wangluo kongjian* [Expert interpretation: Regulate deep synthesis services and create a clean and upright cyberspace]. http://www.cac.gov.cn/2022-12/12/c_1672220143161351.htm

"stitched" not only because of content regulations, but also because of the requirements for the technological architecture of content production/distribution itself.

A separate (and key layer for the Metaverse) is personal data and biometrics. The Chinese data protection regime tightens the requirements for the processing of sensitive information, which in XR ecosystems acquires an ultra-high concentration: motion tracking, facial expressions, gaze, voice impressions, spatial maps of premises, behavioural patterns. Scientific and expert reviews emphasise that PIPL (2021) establishes an enhanced regime for "sensitive personal information", which usually includes biometrics, and also strengthens the requirements for processing grounds and transparency of practices (National People's Congress, 2021; Hu, 2023)[1]. For the dissertation analysis, it is important to note here: in China, privacy in the Metaverse is not an "independent value" in the European sense, but a component of managed data security, which is closely intertwined with state interests and compliance platforms.

In the private law dimension, the PRC is gradually "legalising" the very fact of the existence of virtual assets as an object of interest and protection, which creates the basis for civil law protection of users and businesses in virtual spaces. The norm on the protection of "data and online virtual property" is indicative, which enshrines the fundamental possibility of protecting such objects in accordance with the law (PricewaterhouseCoopers, 2023)[2]. At the same time, in practice, this does not mean "absolute ownership" in the Western sense: the real distribution of powers often depends on platform rules, licences, technical controllability of the asset, and proof of origin (hence the growing role of event logs, identification procedures, and compliance).

The sphere of intellectual property in the Chinese Metaverse has a dual character: on the one hand, the state is interested in protecting the content and technology industry; On the other hand, control of the information space and standardisation can "squeeze" market practices. For XR, this gives rise to the classic problems of object qualification (3D assets, avatars, virtual architecture, scripts, interactive environments) and proving originality/authorship, especially where generative AI or collective creation is used in UGC environments.

Criminal law challenges in the PRC in the Metaverse are structurally similar to other jurisdictions (fraud, account hijacking, illegal access, extortion, invasion of privacy), but differ in the "rigidity of state coercion" and the wider use of administrative-criminal links (when a compliance violation quickly transforms into a case of public danger). In reviews of the criminal law field of the PRC, it is noted that articles on illegal entry/unauthorised access to computer systems can be applied to encroachments on digital platform infrastructure and virtual property (KPMG, 2020)[3]. For XR, this means: proving the event of crime and intent will often rely on the platform's technical logs, identification data, and

1 Hu, X. (2023). The civil law protection of virtual property rights in online games. *International Journal of Frontiers in Sociology, 5*(9), 152–160. https://doi.org/10.25236/IJFS.2023.050925

2 PricewaterhouseCoopers (PwC). (2023, August). *China's interim measures for the management of generative artificial intelligence services officially implemented.*https://www.pwccn.com/en/tmt/interim-measures-for-generative-ai-services-implemented-aug2023.pdf

3 KPMG. (2020, November). *Overview of draft personal information protection law in China.* KPMG Cybersecurity. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2020/11/overview-of-draft-personal-information-protection-law-in-china.pdf

internal event capture systems, and therefore on its willingness to cooperate with the authorities.

Finally, the financial and economic dimension of the Chinese model directly affects what the Metaverse "will be": the state demonstrates a high tolerance for tokenisation only where it is controlled or does not pose systemic risks, and at the same time severely restricts cryptocurrency instruments that undermine monetary and supervisory sovereignty. This is manifested in a consistent line of restricting/suppressing uncontrolled crypto practices, which is regularly recorded in internationally authoritative reviews and news chronicles (Ministry of Industry and Information Technology of the PRC et al., 2022)[1].

China's Metaverse gravitates towards a model of a 'digital economy without crypto anarchy': more industrial VR, fewer open Web3 markets." This is where the main challenge arises: how to combine the speed of innovation with high regulatory density and political and security constraints so that the Metaverse does not turn into a purely "showcase" technology without full-fledged economic self-sufficiency.

The security loop is reinforced by the fact that Chinese cyberspace law has historically built an "architecture of responsibilities" for network operators. For example, the Cybersecurity Law (2017) clearly states that operators must provide technical support and assistance to public security and state security authorities in cases specified by law. For the Metaverse, this has a direct consequence: the platform is not a "neutral environment", but is an entity that is structurally entrusted with the functions of complicity in ensuring cybersecurity (logging, response, access to data according to the procedure, compliance).

The contour of personal data in the PRC has gained special importance after the adoption of the Personal Information Protection Law (2021). The text of the law directly defines the category of "sensitive personal information", which includes, in particular, biometric data; for such information, an increased regime of justification of necessity and special processing conditions are established (National People's Congress, 2021)[2]. In the Metaverse, it is biometrics and behavioural signals that are the core of the XR experience (facial expressions, gaze, movements, voice, "spatial imprints" of the room). Therefore, the Chinese logic of "data as an object of sovereign control" is built into the Metaverse not optionally, but structurally: the XR product architecture must be designed to withstand the legal test of necessity/proportionality and the hypersensitivity regime.

A separate, very "Chinese" layer is the control of information flows and algorithmic infrastructure. For the Metaverse, the modes of oversight of recommendation algorithms (which determine what the user sees and interacts with) and over synthetic/generated content (deep synthesis/deepfake) are crucial. The public materials of the Chinese regulator (CAC) on the rules of algorithmic recommendations emphasise that algorithms are not just "code", but tools that can create public risks, and therefore should be subject

1 Ministry of Industry and Information Technology of the PRC, Ministry of Education of the PRC, Ministry of Culture and Tourism of the PRC, National Radio and Television Administration, & General Administration of Sport of China. (2022). *Action plan for the integrated development of virtual reality and industry application (2022–2026).* https://lawinfochina.com/display.aspx?id=40183&lib=law

2 National People's Congress of the People's Republic of China. (2021). *Personal Information Protection Law of the People's Republic of China (PIPL)* https://appinchina.co/government-documents/personal-information-protection-law-of-the-peoples-republic-of-china/

to the regulatory regime. At the level of generalisation, these principles are well explained in comparative legal reviews (in particular, large law firms that systematise regulatory requirements). For XR, this means: moderation + algorithmic controllability become the "internal constitution" of the Metaverse in the Chinese jurisdiction.

The "deep synthesis" mode is also closely next to it: discussion and explanatory materials on the relevant provisions focus on the labelling/identification of synthetic content, the risks of identity substitution and the danger of manipulation[1]. Public legal commentaries to these rules also emphasise that the state focus is not only in the "ban", but also in the construction of the platform's responsibilities to prevent the abuse of synthetic reality. In the Metaverse, this becomes more acute, because the avatar and synthetic environment are not the exception, but the norm.

On the one hand, the Civil Code of the People's Republic of China recognises that virtual property is subject to legal protection if it is provided for by law. The translation of Article 127 of the Civil Code of the People's Republic of China expressly enshrines the principle: "Virtual property on the Internet shall be protected by law". On the other hand, China consistently maintains a hard line on cryptocurrency transactions and speculation, which directly "hits" the classic Web3 economies of the Metaverse (tokens, crypto exchanges, unregulated circulation). Current media sources record that Chinese regulators continue to view cryptocurrency transactions as illegal and risky for financial stability. Consequently, the Chinese Metaverse tends towards "digital property without crypto sovereignty": virtual assets are protected, but the financial "decentralised" basis of Web3 is significantly limited. (Tian & Zhang, 2024; Karimov, 2024; Kalyvaki, 2023)[2,3,4].

Intellectual property in the Chinese Metaverse tends to be "picked up" by current copyright, related rights, trademark, and technological protection regimes. For the Metaverse, this means: 3D models, virtual architecture, scripts, avatar content, and even "behavioural" digital artifacts are gradually becoming the subject of disputes over authorship, licensing, and legitimate use — but are resolved not by a "special law for the Metaverse," but by a common IP matrix.

The criminal law dimension in the PRC is most consistently manifested in terms of cybercrime and illegal access/circulation of data (Pei, 2024)[5], as well as in the expansion of approaches to accountability for digital manipulation (including deepfake risks, which

1 Cyberspace Administration of China. (2022, December 11). *Dui jizhe wen: "Guanyu hulianwang xinxi fuwu shendu hecheng guanli guiding"*https://www.cac.gov.cn/2022-12/11/c_1672221949570926.htm

2 Tian, X., & Zhang, N. (2024). Controversy of copyright application and the China plan of metaverse products. *International Journal of Digital Law and Governance, 1*, 155–185. https://doi.org/10.1515/ijdlg-2023-0003

3Karimov, E. (2024). Meta-morphosis of copyright and user-generated content: Can East Asia's emerging policies navigate through the metaverse? *Asian Journal of Law and Society.* https://doi.org/10.1017/als.2024.32

4 Kalyvaki, M. (2023). Navigating the metaverse: Business and legal challenges—Intellectual property, privacy, and jurisdiction. *Journal of Metaverse.* https://doi.org/10.57019/jmv.1238344

5 Pei, R. (2024). *Yuan yuzhou beijing xia geren shengwu xinxi de fali bianxi ji baohu lujing* [Legal analysis and protection path of personal biometric information in the context of the metaverse]. *China Law Journal.* https://doi.org/10.55574/yyle6178.

are actively discussed in the public arena) (Yuan, X., & Wang, Z. 2024a; Yuan, X., & Wang, Z., 2024b; Li, Y., 2024)[1,2,3].

At the same time, it is important to emphasise: China often moves not by "inventing new Metaverse crimes", but by transferring existing warehouses to XR environments — if damage, illegality, and evidence can be properly recorded (event logs, account identification, traces of transactions) (Dunmay, 2023)[4]. In this context, the responsibilities of network operators to assist security agencies de facto strengthen the state's ability to carry out law enforcement projection in the Metaverse.

To summarise, Chinese Metaverse regulation can be described as "security-and-standards first": innovation is allowed but built into a rigid framework of oversight of data, algorithms, and content, with the parallel development of the VR/XR industrial base.

The Chinese model actually seeks to make the Metaverse a "state-compliant environment" where the platform's architecture is designed as a compliance engine from the outset (China Briefing, 2023)[5].

1.4. Metaverse Architecture as a Subject of Legal Analysis: Correlation of Technical Layers to Legal Regimes

1.4.1. Metaverse Architecture

Within this subparagraph, the Metaverse architecture is considered not as an engineering scheme of components, but as an infrastructure of legal regimes, in which technical layers give rise to legal facts, rights and obligations, methods of proof and mechanisms of coercion. We propose to describe the Metaverse as a multi-level system: a layer of digital identity and attribution; data layer and access to it; a layer of content and behavioural practices; transactional and economic layer (virtual assets, payments, smart contracts); evidence (audit) layer; layer of sanctions and their application.

It is advisable to describe the technological core of the Metaverse as a multi-level architecture: immersive interfaces (XR) - networks and computing (edge/cloud, low latency) - data and identity (profiles, biometrics, logging) - economic layer (tokens, smart contracts) - algorithmic layer (AI agents, personalisation, content generation). Such a decomposition is important legally, because each layer has its own regime of risks and liabilities: from device security and cyber protection to the personal data mode and the digital asset mode.

In the applied dimension, the Metaverse simultaneously strengthens the possibilities of education and training, industrial modelling and digital twins, medical simulations, commerce and marketing, urban services, and "virtual cities". At the same time, legal challenges are centred around: privacy and biometrics; authorship and IP rights to 3D

1 Yuan, X., & Wang, Z. (2024a). The regulation of metaverse through crime of insult and libel. *OALib.* https://doi.org/10.4236/oalib.1111289.

2 Yuan, X., & Wang, Z. (2024b). The regulation of metaverse through crime of insult and libel. *OALib.* https://doi.org/10.4236/oalib.1111289.

3 Li, Y. (2024). Threats in mixed reality headset use and legal regulation in China: Present and future. *Moscow University Law Bulletin, 11*, 64–72. https://doi.org/10.55959/msu0130-0113-11-64-6-12.

4 Dunmay, P. (2023). Criminal and legal protection of cyber virtual property in modern China. *Gosudarstvo i pravo.* https://doi.org/10.31857/s102694520025200-1.

5 China Briefing. (2023). *China releases three-year action plan for metaverse industry development.* https://www.china-briefing.com/news/china-releases-three-year-action-plan-for-metaverse-industry-development/

content; NFT/tokenised asset regime; interoperability between platforms; fairness of algorithms; evidence of digital traces and attribution of actions. For the dissertation, it is appropriate to directly connect architecture with law: technological modules become "material carriers" of legal regimes, and therefore Metaverse law is inevitably a techno-legal construction.

A study conducted by an international team of scientists (Jim et al., 2023)[1] offers an up-to-date overview, structure, and challenges of the Metaverse. The Metaverse functions through the comprehensive integration of several key technologies (Figure 5):

AI (Artificial Intelligence) — provides content personalisation, automatic creation of a virtual environment, and simulation of user behaviour.

Blockchain — guarantees transparency of transactions, decentralised data storage, ownership of digital assets (for example, NFTs — Non-Fungible Token, non-fungible tokens).

XR (eXtended Reality) - covers VR (Virtual Reality), AR (Augmented Reality) and MR (Mixed Reality).

6G (sixth generation wireless) is the future communication standard that will provide ultra-low latency and ultra-high bandwidth.

Web 3.0 is the concept of a decentralised Internet using blockchain technologies and smart contracts (self-executing contracts).

Big Data is the processing of arrays of behavioural, transactional, and visual user data to adapt content.

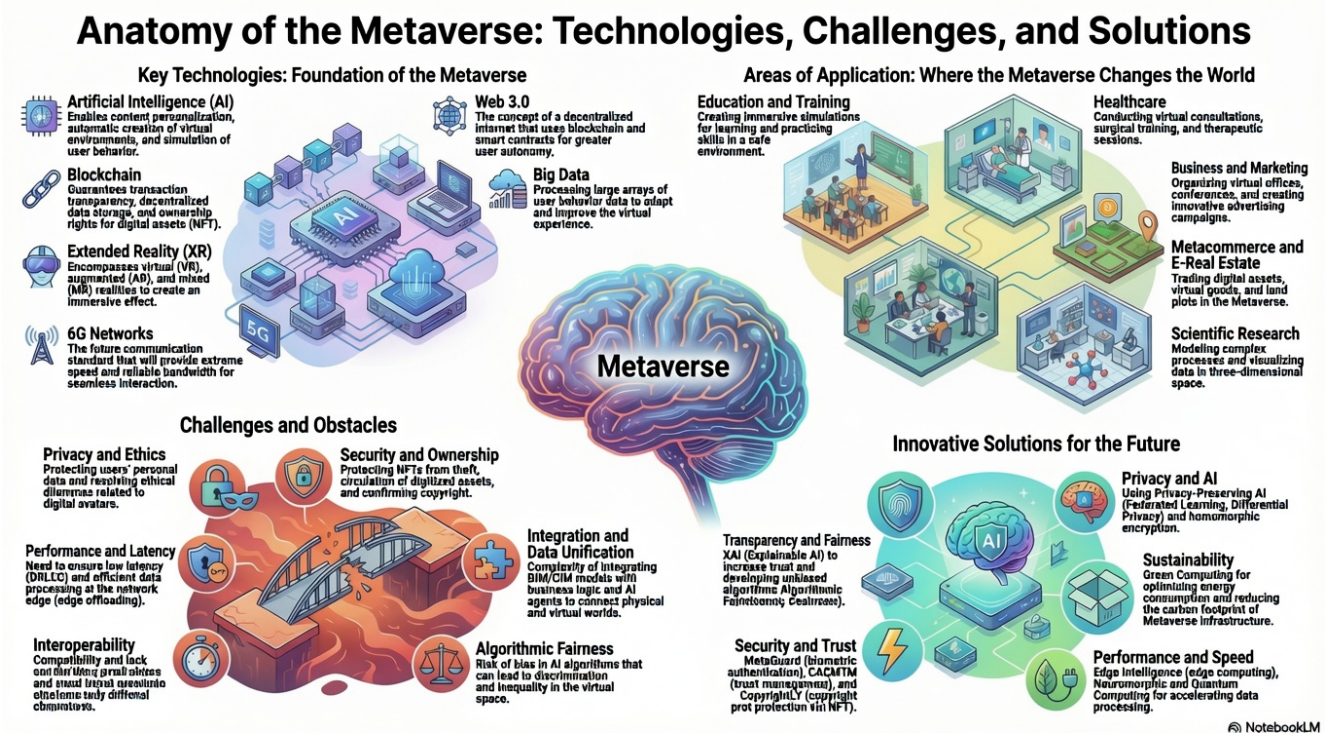


Figure 5. Metaverse: Technologies, Solutions, Challenges.

These components form a multi-layered Metaverse architecture capable of scaling, self-learning, and immersive interaction, as well as define the basic areas of application:

1 Jim, J. R., Hosain, M. T., Mridha, M. F., Kabir, M. M., & Shin, J. (2023). Toward trustworthy metaverse: Advancements and challenges. *IEEE Access.* https://doi.org/10.1109/ACCESS.2023.3304118

education, research and training, healthcare, business and marketing, e-commerce, agriculture, e-real estate. At the same time, the Metaverse cannot but have challenges, such as: privacy and ethics, the circulation of tokenised assets, authorship issues, NFT security, weak interoperability between the Metaverse, fusion of models and systems, the need to unify BIM (Building Information Modeling) and CIM (City Information Modeling) data with blockchain and AI agents to synchronise physical and virtual environments, ensuring low latency URLLC (Ultra-Reliable and Low-Latency Communications) within 6G, and mechanisms edge offloading for near-field servers, lack of AIGC (AI-Generated Content) algorithms for multimodal context recognition, algorithmic fairness and adaptability issues.

At the same time, today, the following list of terms and solutions actually describes the "technological and legal stack" of the Metaverse: from continuous authentication and trust management to privacy, algorithm fairness, explainability, cryptography, computing infrastructure, and environmental sustainability. It is important to immediately fix the methodological framework: some of the names look like designations of research prototypes/concepts, and not mass products; Therefore, when it comes to a specific implementation (architecture, exact modules, metrics), we will rely on generally accepted technical approaches and available references in open sources.

MetaGuard (continuous biometric authentication with Federated Learning) is logically understood as a mechanism that does not "let in" the user once at the entrance, but constantly checks that it is a legitimate subject who uses the XR headset: by head/hand movement patterns, microgestures, voice, gaze dynamics, motor skills, and sometimes by a combination of such signals. The use of Federated Learning in this circuit means that personal biometric raw data should not be centrally "flowing" to provider: model training/update takes place locally on the device or "at the edge" of the network, and only aggregated parameter updates are transmitted to the centre (which reduces the risks of leaks and compliance workload). The term *MetaGuard itself* does appear in open reviews/materials as the name of such an approach to authentication in the Metaverse. Legally, a high-risk array immediately arises here: biometrics and behavioural profiles (in a number of jurisdictions — "sensitive data"), so we need: informed consent, data minimisation, purpose restrictions, profiling transparency, removal procedures, as well as security and re-identification risk audits even in federated schemes.

CACMTM (Context-Aware Cognitive Memory Trust Management) is a class of solutions for trust management in transport cyber-physical systems (V2X, smart roads, autonomous vehicles), where the key is not only "who you are", but also "how much you can be trusted in a specific context". In this logic*, context-aware* means the dependence of trust on the situation (place, time, type of event, riskiness of the scenario), and *cognitive memory* — accumulation of "memory" of previous interactions, sensor data quality, protocol execution history, incidents, and reputation signals. In open publications/mentions, CACMTM is described as precisely a context-sensitive trust mechanism for transport CPS, which methodologically "docks" well with the Metaverse when XR/digital twins of the city are connected to real traffic data streams (National Institute of Standards and Technology, 2023)[1]. The legal node here is responsibility for

1 National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1).* https://www.aigl.blog/nist-ai-100-1-artificial-intelligence-risk-management-framework-ai-rmf-1-0/

decisions made based on the "trust score" (denial of access, priority of messages, blocking nodes), as well as evidence: whether it is possible to retrospectively explain why the system "did not believe" someone and what data/context led to this.

A *similar* architecture as an NFT-based *copyright protection dApp* should be interpreted as a "decentralised outline" of capturing the origin and licensing of digital objects (3D models, avatars, textures, music, scenes, scenarios) in the Metaverse. In scientific/project descriptions, the *Copyrightly* approach is found as a blockchain/semantic-web-oriented decentralised copyright management. An important legal subtlety: NFTs do not "create" copyright, but can only be a technical token (timestamp, provenance, transfer chain) and a tool for automating licence conditions (smart contracts). Therefore, compliance tasks: correct reflection of authorship/co-authorship, derivative works regime, revocation/termination of licences, jurisdiction of disputes, notice-and-takedown procedures, and interaction with platform rules (because moderation/removal of content often takes place centrally, even if the "right" is fixed in a decentralised manner).

Edge Intelligence is the transfer of intelligent computing from the cloud closer to the user (headset, smartphone, home gateway, base station, edge server in the city) to minimise latency, reduce traffic costs, and increase resiliency. For the Metaverse, this is critical because XR requires low latency for rendering, tracking, real-time interaction, and "presence"; therefore, offloading, split-computing, caching, local model execution, and adaptive distribution of tasks between device/edge/cloud. As the review work with Edge AI summarises, "intelligence at the edge" opens up significant opportunities, but it has challenges of security, resource constraints, and model management in a heterogeneous environment (Zhou et al., 2019)[1]. Normatively, this entails the question: where is data processing "located" (transfer across borders), who is the processor/controller, what are the requirements for cyber protection of edge nodes, and how to ensure audit/certification of models, deployed in distributed infrastructure.

Privacy-Preserving AI (FL + DP) should be broken down into two different privacy mechanisms, which are often combined. Federated Learning reduces the need to collect personal data centrally, but it does not guarantee privacy by itself (because it is sometimes possible to draw inverted conclusions from model updates). Differential Privacy adds a formalised guarantee layer: controlled noise, which mathematically limits how much a particular person's participation affects the outcome and how much it can be "deducted". In [2]the Metaverse, the combination of FL+DP is especially relevant for biometrics, body/gaze tracking, and behavioural profiles, because this data is not only personal, but also potentially "irrevocable" (the password can be changed, and the biometric pattern is much more complex). The practical trade-off here is always between privacy and quality: excessive noise reduces accuracy, insufficient — does not give legal/ethical certainty.

Adaptive Context-Aware Interaction and Multimodal Sensory Integration are "interaction intelligence" that makes agents and environments context-sensitive and capable of integrating perceptual channels. The first means that the agent (or interface) takes into account the user's situation: space, activity, social environment, tasks, riskiness, even signs of fatigue or stress — and adapts the hints, the level of intervention, and the

1 Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Revisiting edge AI: Opportunities and challenges. *Proceedings of the IEEE, 107*(8), 1695–1716. https://pure.tudelft.nl/ws/portalfiles/portal/218813846/Revisiting_Edge_AI_Opportunities_and_Challenges.pdf

2 Gentry, C. (2009). *Fully homomorphic encryption using ideal lattices* . STAIR: Stanford Theory Analysis Intelligence & Research. https://ebooks.karbust.me/Technology/Homomorphic%20Encryption%20-%20Paper%20-%20IBM%20Research.pdf

security mode. The second is the synchronous fusion of visual, auditory, and tactile cues to increase the "presence" and accuracy of event interpretation (e.g., when gesture + gaze + voice together form a command). In the legal dimension, these technologies raise the issues of manipulative design, transparency of personalisation, the limits of acceptable neuromarketing, as well as evidence: if the system adapts behaviour to the context, then how to record what exactly it "showed" to the user at a particular moment and why.

Algorithmic Fairness, XAI, and Non-IID Data Handling form a "quality-trust-responsibility" triangle. Algorithmic fairness in a practical sense is the identification and reduction of undesirable systematic biases against groups/attributes (e.g., different accuracy for different demographics or discriminatory consequences in access to services). that make model decisions interpretable for people, which is critical for trust and for legal attribution of responsibility; the NIST approach includes the principles of explainability and related interpretation requirements (National Institute of Standards and Technology, n.d.)[1]. Non-IID data is the "pain point" of distributed learning (especially FL): data from different users/devices is not equally distributed, causing the global model to degrade or become unfair (it works better for "typical" patterns and worse for "marginal" ones). This challenge is widely discussed in federated reviews. For the Metaverse, the consequence is direct: without non-IID strategies (customer clustering, personalisation, domain adaptation, weight correction), it is impossible to consistently guarantee either quality, fairness, or reproducibility.

Homomorphic Encryption, Neuromorphic Computing, Quantum Computing, Reconfigurable Computing, DLT, and Green Computing describe the "deep infrastructure" of the Metaverse. Homomorphic encryption allows calculations to be performed on encrypted data with a correct result after decryption — that is, the computation provider does not see the input data in plain form (Akram et al., 2025)[2]. Neuromorphic computing is aimed at energy-efficient event/sensory processing (potentially useful for XR tracking and on-device inference), quantum computing has a double effect: speeding up some classes of tasks and at the same time putting pressure on cryptography (the need for post-quantum security). Reconfigurable computing (FPGA/adaptive accelerators) makes it possible to change the hardware configuration to meet XR/AI loads in real time. DLT (broadly speaking) supports cross-platform trust, asset, event, and rights registries, but raises questions of jurisdiction, immutability of records, and alignment with the "right to erasure." Green Computing closes the circle: Metaverse, AI rendering, and persistent computing have a carbon price, so optimising energy consumption is becoming not only a technical but also a regulatory requirement (reporting, standards, green compliance).

1.4.2. The principle of legal stratification: "layers" of infrastructure and regimes of law.

It is advisable to consider the principle of legal stratification as a methodological "framework" of legal regulation of the Metaverse, which avoids the false idea of the existence of a "single" universal legal regime for all processes in the virtual environment. In view of the above, the Metaverse is not so much a "space" as a multi-level infrastructure (stack), within which different technical functions give rise to different legal facts, different subject-object relations and, accordingly, different regimes of

1 National Institute of Standards and Technology. (n.d.). *Explainable artificial intelligence (XAI).* https://www.nist.gov/artificial-intelligence/ai-research-explainabilit

2 Akram, S. V., Malik, P. K., Singh, R., Anita, G., Tanwar, S., & Kumar, N. (2025). Security, privacy and trust challenges in the metaverse: A systematic review. *Future Internet, 17*(9), 417. https://doi.org/10.3390/fi17090417

responsibility and protection of rights. That is why "layering" is not a purely technical description; It performs the function of a legal ontology that fixes: where a legally significant event occurs, who initiates or controls it, what evidence it is confirmed, and what is the procedure for its recognition or appeal. Within the framework of this approach, the "layer" of infrastructure should be defined as a relatively autonomous segment of the technological architecture, which:

1) has its own set of operators (identification providers, hosting providers, marketplaces, moderators, payment providers, etc.);

2) forms a specific array of risks (confidentiality, fraud, discrimination, copyright infringement, manipulation of evidence, unlawful sanctions);

3) requires a separate "linkage" of legal means (norms of substantive law, procedural guarantees, technical and legal requirements, compliance).

In other words, stratification makes it possible to build legal regulation as a system of interrelated, but not identical regimes: private law (obligations, property/quasi-ownership, intellectual property), public law (supervision, security standards, administrative procedures), as well as "protocol" (requirements for logging, attestation, cryptographic confirmation of events.

The first is the identity layer, which actually defines the "entrance" to the legal order of the Metaverse. In the legal sense, it constructs subjectivity: who exactly acts (an individual, a representative of a legal entity, an automated agent, an avatar as an interface), in what status and with what degree of tort capacity and responsibility. This raises key issues of attribution of actions (who "signed" the transaction or created the content), authentication and trust services, as well as the limits of acceptable anonymity/pseudonymity. At a practical level, this means that legal regulation should describe not only personal data, but also "identification data" as a separate object of management, including the rules for their collection, storage, transfer and audit. It is on the identity layer that the core of the future Metaverse digital jurisdiction is laid, since without reliable attribution, neither proof, nor fair consideration of disputes, nor enforcement of decisions are possible.

The second is the data layer, which outlines the boundaries of privacy, access and "ownership" of information arrays circulating in the environment. Here, the legal regime usually tends to combine the rules on personal data protection, confidentiality of communications, trade secrets, cybersecurity, as well as contractual terms of use of services. It is important to note that in the Metaverse, data is often sensory and behavioural in nature (biometrics, body movements, voice, microfacial expressions, spatial trajectories), which means that the risks of "de-anonymisation" and secondary use increase. The legal regulation of this layer should include: the principles of data minimisation, target restriction, access control, requirements for logging data transactions and procedures for exercising the rights of the data subject (access, rectification, objection, restriction of processing), and in a format suitable for machine interoperability.

The third is the content layer, which concentrates the regimes of intellectual property, related rights, as well as responsibility for content (including defamation, hate speech, manipulative content, deepfake, pornographic materials, etc.). The peculiarity of the Metaverse is that the content is not only a "file" but also an "event" (performative interaction in real time), which makes it difficult to establish authorship, the fact of

distribution, and the moment of the offence. Here it is important to distinguish: 1) user content; 2) platform content; 3) content generated or modified by AI algorithms; 4) "hybrid" content created in co-authorship of a person and an instrument.

Transparency of moderation rules, notice-and-action procedures, the limits of contractual restriction of user rights and the prevention of "privatised justice" without minimum guarantees of due process are becoming critical for law enforcement.

The fourth is the transactional layer, in which property structures are legally formalised: virtual assets, tokens, digital "things" (quasi-things), intra-platform access rights, licences, rental/use of digital objects, as well as smart contracts as a way to fulfil obligations. This is where compliance reality manifests itself: AML/CFT procedures, KYC/threshold criteria, consumer protection, anti-fraud, rules for returning/disputing transactions, responsibility for technical code errors. It is important that the transactional layer is not reduced to finance: it is also the "access economy" (the right to enter space, the right to use functions, the right to participate in events), and therefore civil law and administrative law regimes are most closely intertwined here.

The fifth is the evidentiary layer, which in the Metaverse has an independent meaning, since any dispute in the digital ecosystem comes down to the question of whether digital footprints can be trusted and how to ensure their admissibility. We are talking about standards of integrity, immutability, reproducibility, traceability, as well as the "chain of custody" of digital evidence. In practice, this means requirements for logging, timestamping, cryptographic hashes, qualified electronic signatures, procedures for exporting/importing evidence from platforms, and even standardisation of metadata. Without normative consolidation of the minimum criteria for "evidentiary operability", the Metaverse turns into an environment with a high level of procedural uncertainty, where a technically stronger entity will always have an advantage over a weaker one.

The sixth is the sanctions layer, which covers moderation, coercion, blocking, access restrictions, "de-platforming", as well as sanctions review procedures. Legally, this is a high-risk zone, because sanctions are often imposed by private operators according to private rules, but their consequences can be commensurate with public law restrictions (loss of access to assets, reputational losses, suspension of economic activity in the virtual economy). Therefore, there is a requirement for procedural legitimacy: notification of the grounds for the decision, the ability to provide explanations, appeal, terms of consideration, proportionality of the measure, prohibition of discrimination, as well as algorithmic transparency in the case of automated detection of violations. In the context of the legal field, it is the sanctions layer that most often demonstrates the gap between the "governance" of the platform and the "legality" of the law, which, in turn, stimulates the development of mechanisms of digital jurisdiction and independent review of decisions (Figure 6).

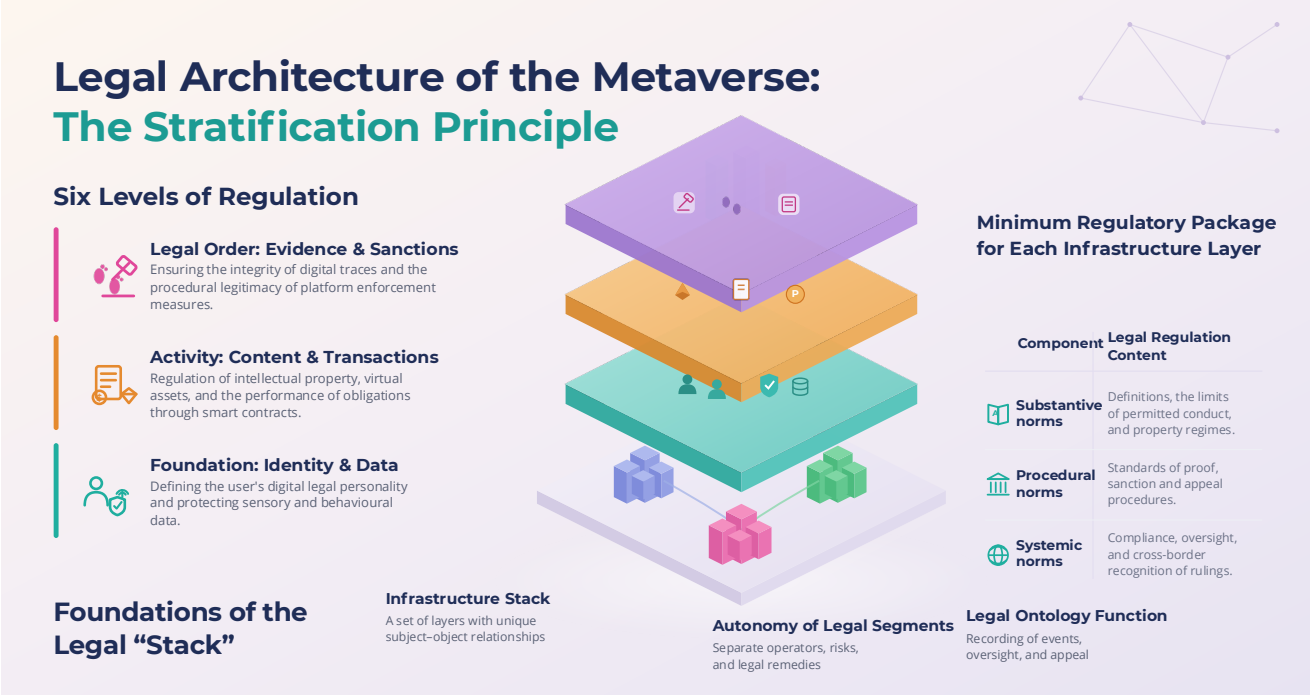


Figure 6. Metaverse: legal ontology.

In summary, the "generalised architecture" of the Metaverse as a legal ontology (Figure 6) should work in the format of a mapping of correspondences: layer - legal facts - rights/obligations - risks - remedies - appeal/recognition procedure. Given the above, this approach allows not only to describe reality, but also to design it normatively: to set technical and legal requirements for protocols, interoperability standards, operator accountability models, and due process guarantees for users. If we formulate an applied recommendation, then each layer should receive its own "minimum package" of norms:

a) substantive legal definitions and limits of what is allowed;

b) compliance and control;

c) evidentiary standards;

d) sanctions and review procedures;

e) cross-border mechanisms of mutual recognition.

It is this stratification, in our opinion, that creates the most suitable basis for further codification of digital law and institutionalisation of digital jurisdiction in multi-entity Metaverse ecosystems.

1.4.3. Digital identity and attribution layer.

Digital identity in the Metaverse performs two interrelated functions: access to the environment and resources; attribution of actions for accountability and proof. For decentralised and portable scenarios, standards for decentralised identifiers and verifiable attributes are important (World Wide Web Consortium, 2022; World Wide Web Consortium, 2025)[1,2].

1 World Wide Web Consortium. (2022, July 19). *Decentralized identifiers (DIDs) v1.0.* W3C Recommendation. https://www.w3.org/TR/did-core/

2 World Wide Web Consortium. (2025, May 15). *Verifiable credentials data model v2.0.* W3C Recommendation. https://www.w3.org/TR/vc-data-model-2.0/

Thus, the EU comparative vector enhances the legal value of "trusted" electronic attestations of attributes and the mutual recognition of means of identification within the European Digital Identity (Regulation (EU) 2024/1183, 2024)[1]. Legally, this allows formalising:

1) levels of identification (anonymity/pseudonymity/personification);

2) the boundaries of legal personality in digital environments;

3) conditions for assigning responsibility for the actions of avatars, agents and "delegated" profiles.

Thus, identity is the primary "entrance" to electronic jurisdiction: without attribution of actions, neither proper procedure, nor evidence, nor sanction is possible, based on the analysis carried out, and also correctly fixes its dual legal nature: on the one hand, it is a tool for access to the environment, services and resources; on the other hand, it is a key mechanism for attribution of actions for the purposes of liability, evidence, and due process.

In the legal dimension, these two functions are not parallel: access without attribution generates a "legal vacuum" (inability to identify the subject of the violation), while attribution without legitimate access turns identity into an instrument of disproportionate control. Therefore, digital identity appears as the primary "entrance" to the digital jurisdiction of the Metaverse, and its architecture should be considered as an element of legal ontology — that is, as a coordinated system of concepts and procedures through which a legal fact arises, is recorded, and becomes suitable for recognition or appeal.

In the context of decentralised and portable identity, technical interoperability is directly translated into legal interoperability. That is why the Decentralized Identifiers (DID) standards and Verifiable Credentials models are in focus. The W3C in the DID specification defines a decentralised identifier as a globally unique and persistent identifier that does not require a centralised registrar, and control over it is cryptographically verified; at the same time, DID methods can (but are not required) to rely on DLT or AI decentralised ledgers.

In turn, the W3C Verifiable Credentials Data Model describes the three-way ecosystem "issuer-owner-verifier" and reveals how claims can be submitted in a machine-readable form, protected from forgery and verifiable in legal relations.

In view of the above, these standards in Metaverse jurisprudence do not serve as a "fashion for Web3", but as a technical and legal basis for the portability of statuses and provable attributes between different platforms.

The EU comparative vector is particularly indicative because it reinforces the legal value of "trusted" attestations of attributes and the mutual recognition of means of identification in the cross-border dimension. The basic logic of mutual recognition of electronic identification is laid down in the eIDAS Regulation No. 910/2014: it directly fixes the principle of mutual recognition of electronic means of identification for access to cross-border online services and introduces assurance levels as a tool for legal "calibration" of risk.

---

1 European Parliament & Council of the European Union. (2024, April 11). *Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. OJ L, 2024/1183, 30.4.2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Further development of this idea took place through Regulation (EU) 2024/1183, which changes eIDAS and forms the European framework for digital identity and wallets (EU Digital Identity Wallet). In a practical sense, this means a shift from "national e-identification for public services" to a broader trust architecture that can work both in the private sector and in cross-border cases. A key element of this development is "electronic attestation of attributes". Even at the level of project logic, the EU formulated their legal effects: the 2021 proposal stipulated that electronic attestation of attributes could not be deprived of legal force and admissibility as evidence only through electronic form, and qualified attestation should be equated in effect to duly issued paper attestations. Following the changes to the current eIDAS regime, these approaches are also specified through a consolidated text that establishes the obligation to ensure that attribute attestations can be obtained, stored and managed within the European Digital Wallet regardless of the state where the wallet is provided (which is a direct norm of "portability" in the legal sense).

Thus, the EU demonstrates an important methodological lesson: identity portability requires not only protocols, but also rules on legal effect, admissibility as evidence, issuance and verification interfaces.

On this basis, it becomes possible to legally formalise the levels of identification and their legal consequences. It is not just about the "anonymous/not" scale, but about normatively defined regimes: anonymity as an acceptable regime for low-risk actions; pseudonymity as a compromise between privacy and attribution (through verifiable attributes without full disclosure of identity); personification as a regime of increased trust for transactions that entail property and/or public law consequences. It is important that eIDAS operates with levels of trust (low/substantial/high), and this allows building a "legal bridge" between technical authentication mechanisms and the requirements of law for proper identification (Figure 7).

It is this "gradation" that is more suitable for the Metaverse than binary logic, as it gives the right a tool of proportionality between privacy, security, and responsibility.

Further, legal stratification of identity makes it possible to outline the boundaries of legal personality in digital environments. Metaverse practice gives rise to multi-layered roles: a person as the primary bearer of rights; avatar as a presence interface; "delegated profile" (for example, business or family sharing); an automated agent (bot/AI agent) that executes commands or acts according to predetermined logic. It is legally important not to confuse these levels: an avatar is not an independent subject of rights (today), but can be a "means of performing actions", and therefore requires an attribution regime similar to representation or use of a tool. Verified attributes (status of majority, professional qualifications, powers of a representative, etc.) become a kind of "procedural keys" of admission to certain legal regimes and procedures.

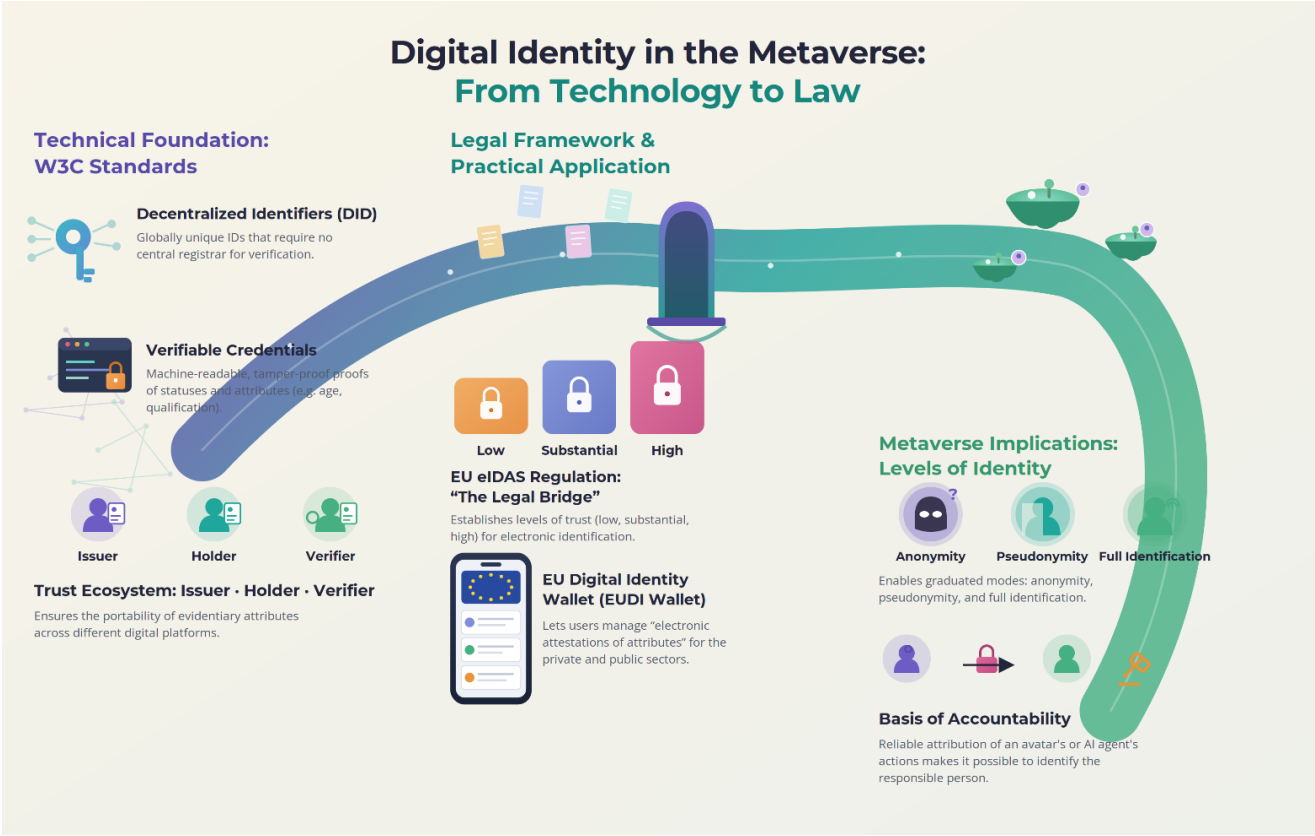


Figure 7. Metaverse: digital identity.

The third point requires a separate deployment — the conditions for assigning responsibility for the actions of avatars, agents, and delegated profiles. If the identity infrastructure provides reliable attribution, the right gets the ability to distinguish: actions performed directly by the user; actions committed by the representative within the limits of delegated powers; Actions initiated by an automated agent, but controlled by the user (through settings, access policies, signing keys, event logs). Evidence of control and intent becomes especially important here: who had access to the keys/account, what delegation policies were in place, whether there was a security breach, whether there were mechanisms for revocation of authority.

In the European approach, this correlates with the idea of qualified attestations and their legal effect, since they create a "trusted layer" of confirmation of statuses and powers relevant to liability. Thus, identity is the primary "entrance" to electronic jurisdiction and this is methodologically and legally justified. Without attribution of actions, it is impossible to ensure due process (who is the addressee of the claim and who has the right to defence), it is impossible to form an evidence base (what exactly happened and by whom), and it is also impossible to legitimately apply sanctions (because a sanction without identifying the subject turns into an arbitrary restriction of access). This conclusion is consistent with both the general logic of eIDAS on mutual recognition and trust levels, and with the newer EU framework on digital identity wallet and electronic attribute attestations, based on the analysis carried out.

1.4.4. Data layer: privacy, cybersecurity, logging.

The Metaverse forms extremely intensive data flows (including biometric, behavioural, spatial), which increases risks to privacy, discrimination, and information security. For example, in EU law, a new wave of data regulation is reflected in the Regulation (EU) 2023/2854, 2023)[1], which, along with the regimes of personal data protection, sets the framework for the redistribution of control over data between manufacturers/providers/users. It is important to capture: who is the "controller" and "processor" of data in the multi-subject virtual world; what are the grounds for access to data (contractual, legal, public law); What are the guarantees of data integrity and minimisation. This is where the technical and legal prerequisites for trust are laid: without data guarantees, there is no legitimate evidentiary trail and the accountability of the platform does not work, given the above.

The intensity of data flows is a legally determining circumstance: we are talking not only about "ordinary" registration data, but about continuous arrays of behavioural, spatial and often biometric signals (trajectories, gestures, parameters of interaction with the environment, device telemetry, attention indicators, etc.). Such a density of collection and processing increases the risks of privacy violations, unfair profiling, and discrimination, as well as expands the plane of information security: the vulnerability of the data flow in XR/IoT chains can be transformed into a vulnerability of a person's legal status, property interests, and procedural safeguards.

For example, EU law forms a dual regulatory framework "complementary layers" of legal data regulation. The first layer is the GDPR as a fundamental regime for personal data protection, which defines the concepts, principles, grounds for lawfulness of processing and accountability. The second layer is the Data Act (Regulation (EU) 2023/2854) as a horizontal regime of "fair access to data and use of data", which aims to redistribute control over data in the data economy and establish conditions for access/transfer of data between market participants and, in exceptional cases, the public sector; The regulation applies from September 12, 2025 (with transitional provisions for individual duties).

A key legal novelty of the Data Act is the regulation of relationships around data generated during the use of connected products and related services, and the clarification of roles (in particular, "data holder") and the user's rights to access such data and the ability to transfer it to third parties. EUR-Lex in a summary explicitly emphasises the focus of the regulation on the "fair distribution of the benefits of data", the definition of "who can use which data and on what terms", as well as on the mechanisms of portability and contractual fairness in data-sharing relations. In the context of the Metaverse, this means that "control of the footprint" ceases to be an exclusively technical prerogative of the provider: it becomes the subject of a legal division of powers between the manufacturer/provider, the service operator and the user if the data flow arises from the use of connected devices and related digital services. At the same time, it is fundamentally important to methodologically record that the Data Act does not replace the personal data

1 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). (2023). *Official Journal of the European Union,* L series. http://data.europa.eu/eli/reg/2023/2854/oj

protection regime, but functions "next to it" and within its limits. The European Commission explicitly emphasises the compatibility of the Data Act with the GDPR and that when the requested/transferred data contains a personal component, it is possible to provide it only if there is a proper legal basis (e.g. consent) – especially in cases where the user requesting the data is not the subject of personal data.

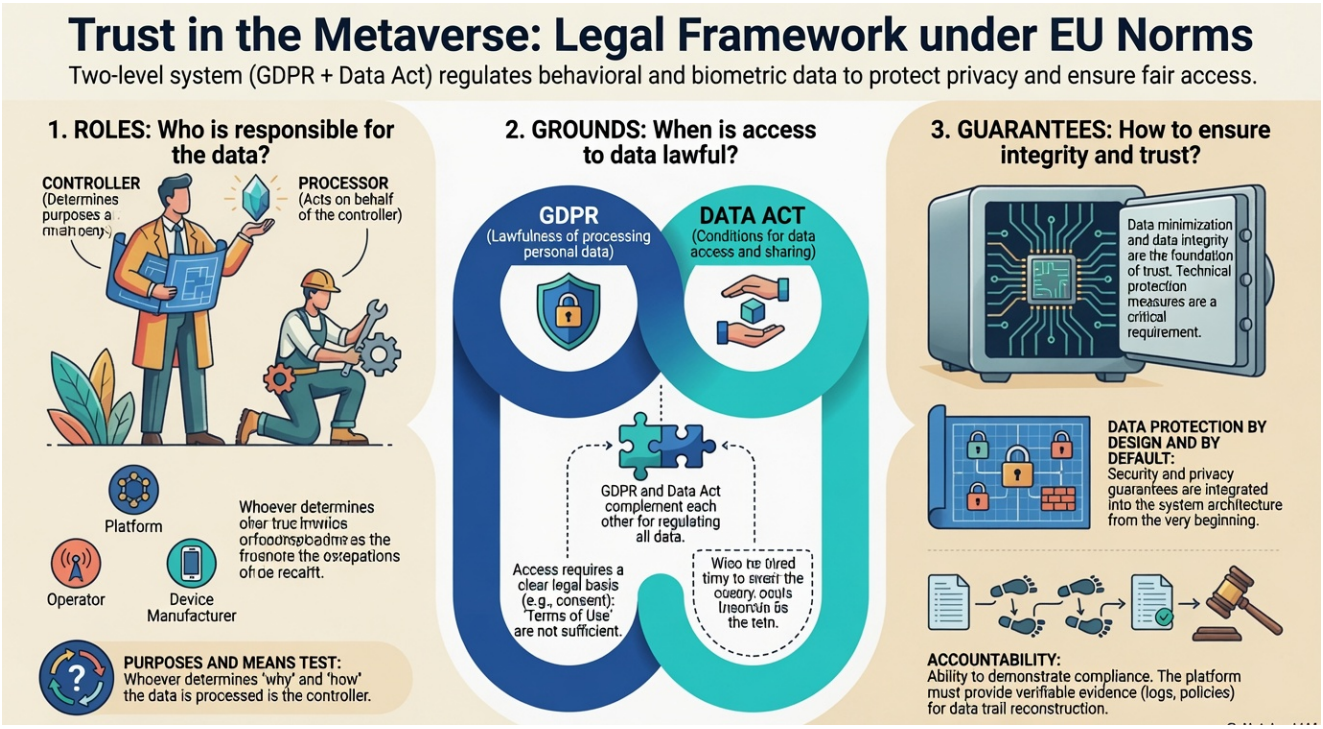


Figure 8. Metaverse: GDPR.

Therefore, for the Metaverse, where data is often "mixed" (personal/non-personal, co-generated), the legal analysis should proceed from the priority of the GDPR for the personal segment and the correct "stratification" of the legitimacy of access/exchange of data (Figure 8).

That is why in a multi-subject virtual world, it is critically important to establish exactly who is the "controller" and the "processor". The GDPR defines a controller as an entity that independently or jointly determines the purposes and means of processing, and a processor as someone who processes data on behalf of the controller.

The practical implication of this definition for the Metaverse is that the "platform" is not always a single controller: controller functions can be distributed (shared controllers) between a Metaverse operator, an XR device/OS provider, a developer of a separate virtual space, or an analytics service — depending on who determines *why* and *how* data are processed. In such a situation, it is advisable to use the "goal and means test" as a basic tool for the legal qualification of roles: if the actor forms the purpose of processing (personalisation, security, targeting, compliance) and determines the key parameters of the technological circuit (data categories, storage periods, access rules), he gravitates towards the status of a controller or co-controller.

The second position is the grounds for access to data (contractual, legal, public law). In the GDPR, the lawfulness of processing is tied to one of the grounds of Article 6

(consent, contractual necessity, legal obligation, vital interests, public interest/authority, legitimate interest).

The Data Act, for its part, establishes the conditions under which a "data holder" may be obliged to provide data to another business, provides for rules of contractual fairness, as well as a mechanism for requesting data by public sector bodies in situations of "exceptional need" (including during extraordinary circumstances).

This leads to an important legal conclusion: in the Metaverse, access to data cannot be justified by "terms of use" alone; it must be related to the proper basis and correct role of the subject in the data processing/provision relationship.

The third position — guarantees of data integrity and minimisation — is not a decorative "privacy block", but the core of the Metaverse's evidentiary and managerial capacity. The GDPR enshrines the principles of data minimisation and integrity and confidentiality, and also directly establishes that the controller is responsible for compliance with the principles and must be able to demonstrate this (accountability).

Additionally, Article 25 of the GDPR requires "data protection by design and by default", i.e. the integration of minimisation and guarantees into the processing architecture itself at the stage of determining the means.

In the Metaverse plane, this means that technical means (access logs, version control, cryptographic integrity mechanisms, access rights segmentation, storage policies) should be legally "readable" as the implementation of regulatory principles, and not as an internal engineering convenience.

This logically follows your final thesis about the technical and legal prerequisites of trust. If data is not minimised, protected, and tracked, then the "digital footprint" becomes either excessive (creates illegality/disproportionality) or unreliable (raises doubts about reliability), and therefore cannot serve as a legitimate basis for proof and accountability. In this place, it is appropriate to show that the platform's accountability in the GDPR paradigm is not a declaration, but the ability to prove compliance with the principles of processing, including security and purpose limitation.

It is in the Metaverse that accountability acquires a "protocol" character: the platform must be able to provide verifiable artifacts (log events, policies, records of access decisions) that allow you to independently reconstruct the path of data from generation to use.

Finally, the regulation is not only about "sharing access", but also about increasing legal certainty and competition in data infrastructure, in particular through the rules on the transition between providers of data-processing services (cloud switching) and the restriction of unfair contractual terms.

For the Metaverse, where data and services are often "locked" to a single provider, this opens up an important regulatory horizon: reducing the dependence of users and businesses on monopoly conditions and the emergence of structural incentives for interoperability.

The obvious fact is that legal data regulation in the Metaverse should simultaneously: define the roles of the controller/processor (and, if necessary, joint controllers) according to the criterion of "goals and means"; align the grounds for access/data exchange with the GDPR and the Data Act mechanisms; institutionalise

guarantees of minimisation and integrity as a measure of the procedural legitimacy of the evidentiary trail.

It is this triangle — the role → basis → guarantee — that forms technical and legal trust, without which electronic jurisdiction in Metaverse ecosystems turns into a declaration rather than a workable mode.

1.4.5. Content and behaviour layer: moderation, responsibility, IP.

Content in the Metaverse (including UGC, "spatial" objects, audiovisual streams, generative content) is the core of social implications and the subject of intense scrutiny. The EU regulatory logic enshrined in the Digital Services Act (Regulation (EU) 2022/2065, 2022) [1] forms a matrix of responsibilities of intermediary services: transparency of moderation, reporting and response mechanisms, justification of restrictions, internal complaint handling systems, and risk auditing. This effectively "translates" moderation into the categories of due process: notification, motivation, possibility of appeal, proportionality of sanctions. A separate block in this layer is the intellectual property of digital objects and the modes of its protection, since it is here that typical conflicts arise regarding authorship, licences and derivative works, in view of the above.

In the Metaverse, content (UGC, "spatial" 3D objects, real-time audiovisual streams, as well as generative products) is not just a "content" of the platform, but a legally relevant social interaction environment in which conflicts of rights, competition of jurisdictions, and litigation practices arise. The legal complexity of this layer lies in the fact that content is simultaneously an object of civil rights (primarily intellectual property), a channel for the dissemination of potentially illegal information, a trigger for administrative and procedural decisions of platforms (moderation, blocking, restriction of functions), which de facto have a sanctioning effect. That is why the normative "optics" of content in the Metaverse should be built as a combination of material regimes (what is prohibited/allowed) and procedural guarantees (how exactly the decision is made and reviewed).

In this sense, the EU logic enshrined in the Digital Services Act (Regulation (EU) 2022/2065) forms a matrix of responsibilities for intermediary services and online platforms working with user content. The DSA builds a "cascade" of responsibility: from general requirements for transparency of rules and restrictions to formalised procedures for reporting and responding to illegal content; From minimal guarantees for users to special responsibilities of large platforms for system risk management and independent auditing. In fact, the DSA sets the framework for "regulated self-governance" of platforms, where private rules and moderation decisions should be procedurally ordered and accountable, rather than purely discretionary.

The most fundamental thing is that DSA allows moderation to be "translated" into the category of due process in digital environments. Such a translation means that any restriction of content or account cannot be considered as a technical action of the "administrator", but must be qualified as a solution that:

1 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). (2022). *Official Journal of the European Union,* L 277, 1–102. http://data.europa.eu/eli/reg/2022/2065/oj

1) addressed to a specific recipient of the service;

2) has a basis (illegality of the content or non-compliance with the terms of use);

3) gives rise to legal consequences for the rights and freedoms of the user (access, reputation, economic interests);

4) therefore, it requires minimal guarantees — notification, motivation, the possibility of appeal and review.

The DSA explicitly institutionalises such safeguards, in particular through requirements for appeal and alternative dispute resolution procedures for moderation decisions. In the applied context, the "matrix of responsibilities" of the DSA for the content layer can be reduced to several nodal tools of their application.

First, these are notice-and-action mechanisms that standardise the interaction between the applicant, the platform, and the content author/distributor.

Secondly, it is the obligation to provide the user with a clear justification for the restriction (statement of reasons), which reduces the risk of "secret" moderation and creates an evidentiary base for appeal.

Thirdly, these are internal systems for considering complaints and the possibility of applying to certified bodies for out-of-court settlement, which actually forms a procedural "ladder" for the protection of rights within the platform environment.

Special attention should be paid to the risk-based component of DSA, which is critically important for the Metaverse as an environment of high intensity of interactions and rapid cascading effects (mass raids, manipulations, coordinated campaigns, deepfake attacks on reputation, etc.). The Regulation provides for obligations for the largest platforms to assess systemic risks and undergo an independent audit of compliance with DSA requirements; Methodologically, this shifts the content layer from the mode of reactive response to complaints to the mode of preventive risk management. In our opinion, it is risk management and audit in DSA that allows the law to influence not only the consequences (deletion/blocking), but also the architecture of recommendation systems and moderation processes that produce conflicts in the Metaverse.

It should be emphasised that intellectual property in the Metaverse is not an additional topic "next to moderation", but a structural element of the content layer, because it is here that typical conflicts over authorship, licensing, and derivative works are concentrated. The European legal framework for copyright (in particular Directive 2001/29/EC — "InfoSoc") enshrines the fundamental logic of protecting works in the digital environment, including reproduction and communication to the public, which is directly relevant for the publication of 3D objects, textures, music, videos, and streams in the Metaverse.

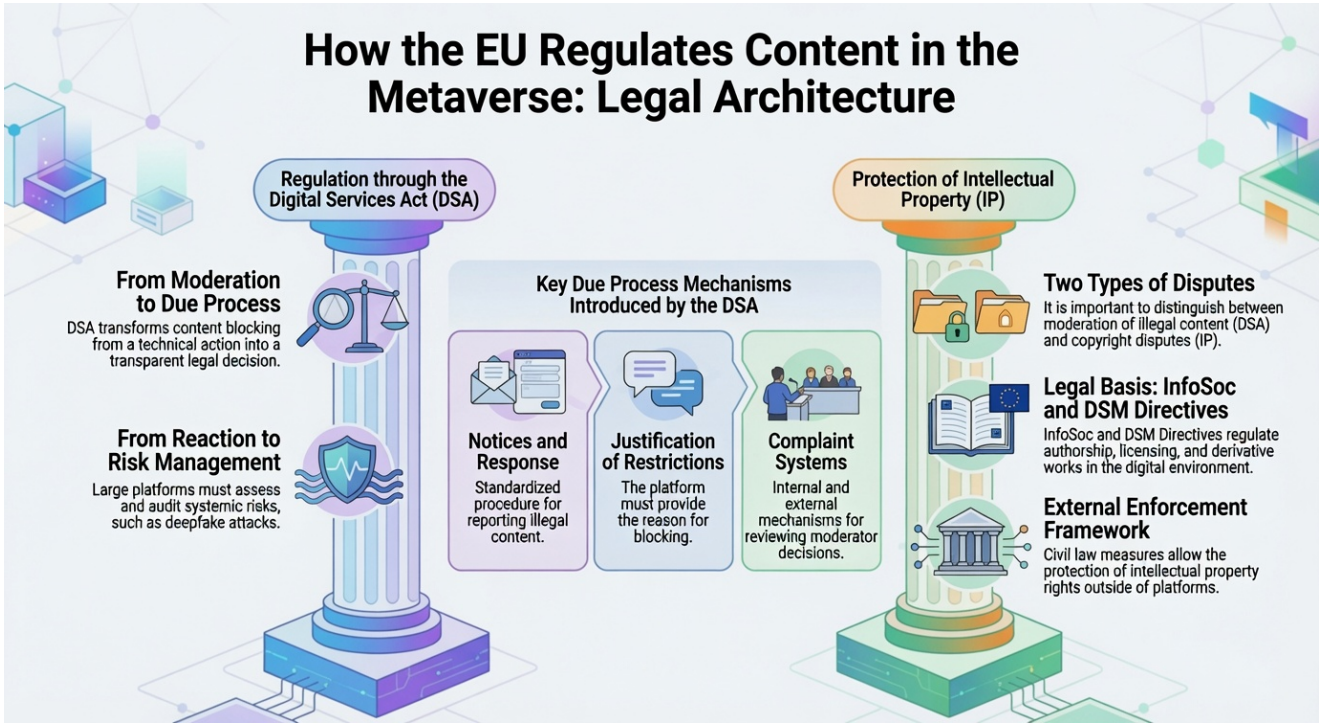


Figure 9. Metaverse: content regulation.

At the same time, the regime of Directive (EU) 2019/790 (DSM) is particularly significant for UGC platforms, in particular its approach to online content distribution services: it shifts the focus from a purely "hosting neutrality" to a liability/licensing model, where platforms must make "best efforts" to obtain copyright holders' permissions and respond appropriately to claims of infringement, but at the same time provide safeguards for legitimate use (exceptions/restrictions) and complaint and redress mechanisms (Figure 9).

The EU Commission, in its guidelines on the application of Article 17 of the DSM, emphasises the need to balance the need to balance effective protection of rights and the prevention of excessive blocking of legitimate content, which for the Metaverse is actually a matter of "procedural fairness" in the moderation of copyright complaints. An important methodological position follows from this: in the Metaverse, it is advisable to distinguish between the moderation of "illegal content" in the sense of DSA and dispute enforcement in the field of copyright and related rights, where the key are licensing structures, identification of the object of protection, establishment of authorship/succession, and derivative works.

Typical conflicts here are of a "trigger" nature: the same 3D object can be both a UGC, part of a common space, and a derivative of a protected design; A single stream can contain music/visuals with different legal regimes. Therefore, due process in copyright cases should include not only quick deletion, but also correct verification of claims, transparent licensing rules, and effective mechanisms for denying and restoring content in case of erroneous blocking.

Finally, the content layer needs effective means of protecting rights outside of internal platform procedures, since not all disputes can be correctly resolved "inside" the ecosystem. In EU law, Directive 2004/48/EC on the enforcement of intellectual property rights establishes a minimum set of civil law measures and remedies (procedures,

evidence, orders, redress, etc.), which forms an external "coercive circuit" for cases of systemic violations. In view of the above, it is a combination of: DSA moderation and appeal procedures; substantive copyright rules (InfoSoc/DSM); mechanisms of civil enforcement and enforcement (IPR Enforcement) — creates a holistic architecture of legal regulation of content in the Metaverse and makes this layer suitable for digital jurisdiction, based on the analysis carried out.

1.4.6. Transactional-economic layer.

The Metaverse architecture includes payment and exchange mechanisms, marketplaces, tokenised objects, as well as smart contracts as a tool for automating the execution of conditions, regulated under EU rules on markets in crypto-assets (Regulation (EU) 2023/1114, 2023)[1]. The transactional layer itself makes it necessary to clarify the rules of jurisdiction, applicable law, and enforcement of decisions in the digital environment, since the dispute acquires a "value" dimension and goes beyond internal moderation.

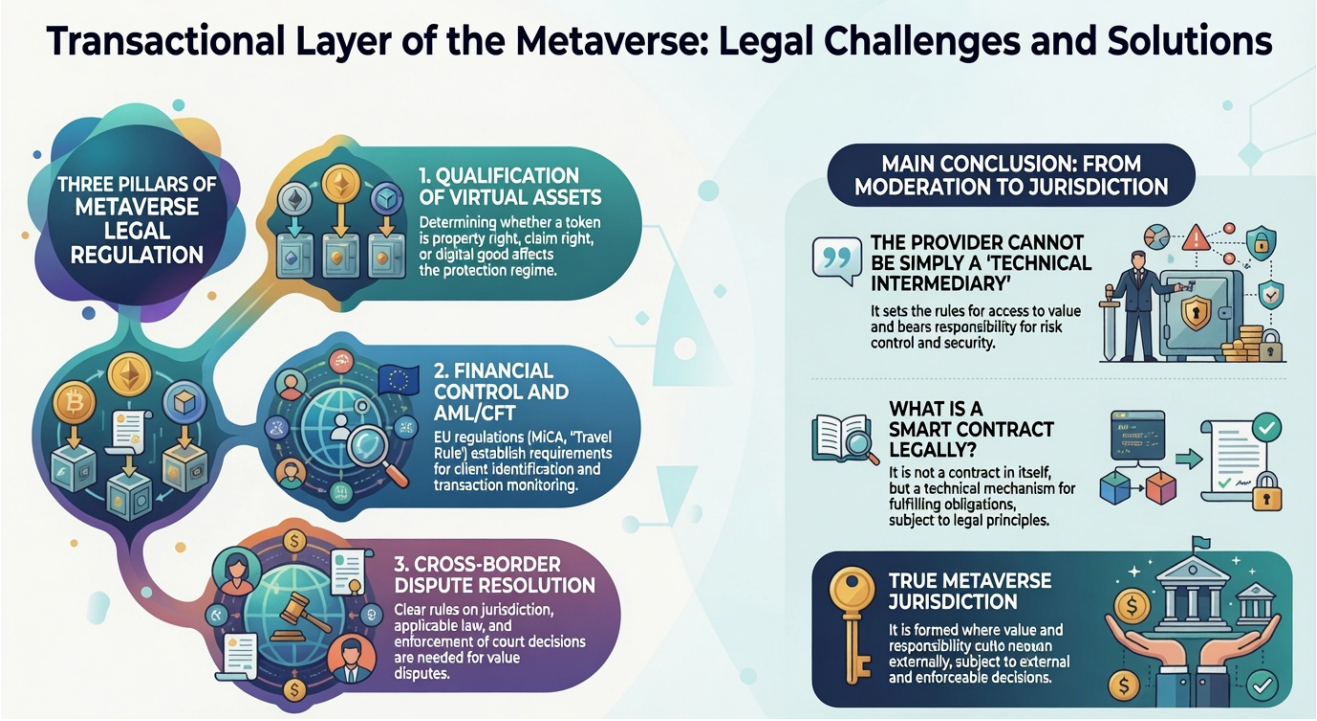


Figure 10. Metaverse Transactional Layer.

The Metaverse transactional layer — payment and exchange mechanisms, marketplaces, tokenised objects, smart contracts — is the part of the infrastructure that transfers user interaction from the plane of "communication and content" to the plane of property legal relations. It is here that digital actions acquire a value dimension, and therefore the legal qualification of events ceases to be purely "platform" (internal rules, moderation) and begins to be subject to the requirements of private and financial law,

1 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Markets in Crypto-Assets Regulation – MiCA). (2023). *Official Journal of the European Union*, L 150, 40–205. http://data.europa.eu/eli/reg/2023/1114/oj

compliance, as well as cross-border rules of jurisdiction and enforcement of decisions (Figure 10).

Legally, the primary task is to establish the legal nature of virtual assets and related competencies. In the Metaverse, the same tokenised object can function as:

a) property right (for example, the right to alienate or use a digital resource);

b) right of claim (creditor's claim against the issuer or service provider);

c) "digital good/service" in the contractual access design, or

d) a tool for participation in the ecosystem (utility logic).

The protection regime (civil, consumer, financial), the admissibility of certain automation mechanisms (smart contract as a method of execution, not as a "self-sufficient contract"), and the limits of responsibility of the platform operator and intermediaries depend on the correctness of this qualification.

In EU law, this regulatory array is systematised, in particular, in Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), which forms uniform rules for crypto-assets and related services at the Union level.

It is important that MiCA not only describes the categories of crypto assets and the requirements for their issuance/offer, but also lays a framework for the activities of crypto-asset service providers and information disclosure standards (in particular through white papers), which is directly relevant for Metaverse marketplaces and exchange/exchange mechanisms. From a regulatory standpoint, the MiCA application calendar is also indicative: general applicability from December 30, 2024, and separate rules for asset-linked tokens and e-money tokens from June 30, 2024, demonstrating the priority of more stable "quasi-monetary" segments in the EU's risk-based logic. The second plane of the transactional layer is the limits of applicability of financial regulation and AML/CFT control. Where a virtual asset performs a payment or investment function or is used to exchange value, the importance of regulations on customer identification, transaction monitoring, travel rule, and countering financial abuse is increasing. In the EU, these requirements are reinforced, in particular, by Regulation (EU) 2023/1113 on information accompanying transfers of funds and transfers of certain crypto assets, which explicitly establishes rules for data on the initiators and beneficiaries of crypto transfers for the purpose of preventing money laundering and terrorist financing. It is significant that the AML logic of the new wave directly "stitches" MiCA and travel rule: AML Regulation 2024/1624, among other things, refers to expanding the traceability of crypto asset transfers and covering relevant providers with AML requirements as obliged entities. The third plane is the liability regimes of providers and intermediaries in Metaverse transactions. The property segment does not tolerate "vague" liability: criteria are needed: who is the issuer, who is the service provider (storage, exchange, placing orders, managing the trading platform), who is the technical operator of the smart contract, and who is only a hosting intermediary. That is why MiCA, through the requirements for the activities of crypto service providers and through transparency standards (including format requirements for white papers and requirements for keeping records in certain segments), forms a legal "profile of good behaviour" for market participants, which in Metaverse practice should be reflected as a compliance outline of the marketplace/exchange/exchanger.

The "transactional layer provider" in the Metaverse cannot be reduced to the role of a "technical intermediary", since it organisationally determines the rules for access to value, the procedure for executing transactions, and often the conditions for storing assets; Therefore, its responsibility should be evaluated according to the criteria of risk control, information and security, and not only by formal status.

A smart contract needs special attention as a tool for automating the fulfilment of conditions. In the legal plane, it is correct to consider a smart contract not as a "contract that exists by itself", but as a technical mechanism for fulfilling or securing obligations, which can accompany contractual terms (human-speaking) and implement them in code. This gives rise to typical issues of dispute enforcement: code error, non-compliance of the code with the agreements of the parties, defects of will (delusion/coercion), consumer protection, consequences of force majeure, as well as the possibility of "stopping" or "rollbacking" enforcement in case of fraud. It is legally appropriate to emphasise that automation does not cancel the basic principles of private law (propriety of consent, good faith, proportionality of responsibility, restitution), but only transfers their implementation to the protocol environment, where additional safeguards and audits are required.

It is the transactional layer that makes it inevitable to clarify the rules of jurisdiction, applicable law, and enforcement of decisions in the digital environment, because the dispute goes beyond "internal moderation" and requires external coercion. Within the EU, the key instruments here are, firstly, Regulation (EU) No. 1215/2012 (Brussels I bis) on jurisdiction and recognition/enforcement of judgments in civil and commercial matters, which sets the procedural infrastructure for cross-border dispute enforcement.

Secondly, Regulation (EC) No 593/2008 (Rome I) on the law applicable to contractual obligations, which legitimises the autonomy of the will of the parties, but at the same time limits it to mandatory rules and rules for the protection of the weak party in the relevant categories of contracts. Thirdly, Regulation (EC) No. 864/2007 (Rome II) for non-contractual obligations (torts), which becomes relevant for non-contractual liability in case of fraud, misappropriation of an asset, violations of competition rules or certain types of damage.

As a result, the transactional layer in the Metaverse requires not just "rules of use", but a legally interoperable model: clear contractual structures (terms of service, execution procedure, return/challenge procedures), definition of the competent forum and law (choice of court / choice of law, taking into account imperative restrictions), evidentiary procedures (transaction protocols, access logs, cryptographic confirmations), mechanisms for executing decisions outside the platform. It is at the intersection of MiCA compliance and private law conflict of laws regimes that the "real" digital jurisdiction of the Metaverse is formed: it begins where cost and liability require an external, verifiable, and enforced decision, and not just the platform as an arbiter of its own rules.

Therefore, the Metaverse transactional layer is the legal point of crystallisation of three interconnected blocks:

1) qualification of virtual assets and powers in relation to them;

2) financial-regulatory and AML/CFT control, which is reinforced by MiCA and "travel rule" regime;

3) cross-border procedural architecture (jurisdiction, law, enforcement),

4) without which the dispute over digital value has no effective legal conclusion. In this logic, internal moderation is only auxiliary, while full-fledged legal regulation should ensure the accountability of providers, the evidentiary capacity of transactions, and the real enforceability of decisions in the digital ecosystem.

1.4.7. Evidence (audit) layer.

For digital jurisdiction, the key is not the fact of the availability of technical logs, but their procedural suitability: the ability to identify the source, confirm integrity, recreate the chain of custody and ensure verifiability. National standardisation in the field of digital evidence is reflected in DSTU EN ISO/IEC 27037:2022, which establishes guidelines for the identification, collection and preservation of digital evidence (DSTU EN ISO/IEC 27037:2022, Modern[1] Ukrainian research also details the criteria for the admissibility of electronic evidence and the components of the proper way to obtain it (Romaniuk, 2024)[2]. A separate dimension is the use of VR for the reconstruction of events and the presentation of evidence in court proceedings, which actualises the requirements for authenticity and procedural guarantees (Heetkamp & Bohatchuk, 2025)[3].

It is advisable to conceptualise the audit layer in the Metaverse as an institutional-procedural circuit that ensures the transformation of the "digital footprint" into procedurally usable evidence. What is fundamental here is not the very fact of the existence of logs, telemetry or event logs, but their ability to withstand verification in the competitive procedure: identification of the source, confirmation of integrity, fixation of the context of formation, as well as the possibility of reproduction and independent verification. In view of the above, the audit layer is the "jumper" between the technical infrastructure of the Metaverse and the electronic jurisdiction, without which no event (transaction, moderation decision, avatar actions, change of a digital object) acquires the proper evidentiary value.

In the legal sense, the procedural suitability of digital evidence should be expanded through the classical criteria of evidentiary law: propriety, admissibility, reliability and sufficiency. For the digital environment, these criteria are "translated" into more specific technical and legal requirements:

1) origin (provenance) and the ability to identify the primary source of the event;

2) integrity, which is confirmed by checksums, cryptographic signatures, impossibility of discreet editing;

3) authenticity — compliance of the evidence with the event/object claimed by the party;

4) reproducibility — the ability to re-obtain/verify the same result by an independent subject. In this regard, it is fair to emphasise: if the platform cannot provide verification artifacts (metadata, access logs, shaping protocols, version control mechanisms), then even "full logs" become legally vulnerable.

1DSTU EN ISO/IEC 27037:2022. (2022). Guidelines for the identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012, . https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100063

2 Romaniuk, V. V. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Pravo i bezpeka.* https://pb.univd.edu.ua/index.php/PB/article/view/818

3 Heetkamp, S., & Bohatchuk, D. (2025). Virtual reality in judicial proceedings: *A view from Germany and Ukraine.* https://www.researchgate.net/publication/394576579_Virtual_reality_in_judicial_proceedings_a_view_from_Germany_and_Ukraine

The regulatory framework for a standardised approach to the processing of digital evidence in the national dimension is reflected in DSTU EN ISO/IEC 27037:2022, which is directly positioned as a guideline for identifying, collecting, acquiring and preserving digital evidence, with a focus on maintaining its integrity.

The importance of this standard for the Metaverse lies in the fact that it sets universal "checkpoints" for the life cycle of evidence: from the initial identification of a potentially relevant source to the procedures for its extraction and conservation in a state suitable for further research and forensic evaluation. In an applied way, this means: the audit layer should be designed so that each significant event is not only recorded, but also "packaged" in a format consistent with the principles of proper handling of digital evidence.

The chain of custody category itself should be reproduced in the Metaverse not declaratively, but as a documented and technically verifiable route of proof: who, when, and on what basis accessed; what operations were performed (copying, exporting, format conversion); where and in what way the storage took place; what integrity controls are used; who carried out verification and when.

In our opinion, in disputes, the Metaverse chain of custody should include another mandatory element: the chain of interoperability, that is, a description of how exactly the evidence was transferred between systems (platform → forensic storage → expert → court) without losing metadata and without "breaking" the context of the event. It is interoperability gaps (loss of timestamps, session IDs, information about the environment version) that most often turn technically convincing material into procedurally vulnerable.

Additional legal certainty for the Ukrainian process is provided by the fact that electronic evidence is expressly enshrined in national procedural codes as information in electronic (digital) form, including electronic documents, web pages, messages, metadata, databases, etc.

At the same time, this formal certainty does not cancel the problem of admissibility: it is important for the court *how the* evidence is obtained, *whether* its immutability is ensured, *whether the* rights of the parties are not violated, and *whether* its origin and integrity can be verified.

In view of the above, the scientific and practical discussion in Ukraine is naturally shifting from the question "whether this is electronic evidence" to the question "under what conditions it will be admissible and convincing". Indicative here are the benchmarks that in the Ukrainian academic and methodological field are associated with the approaches of the Council of Europe to electronic evidence: emphasis is placed on the evaluation of electronic evidence according to common criteria, with a focus on authenticity, accuracy, integrity.

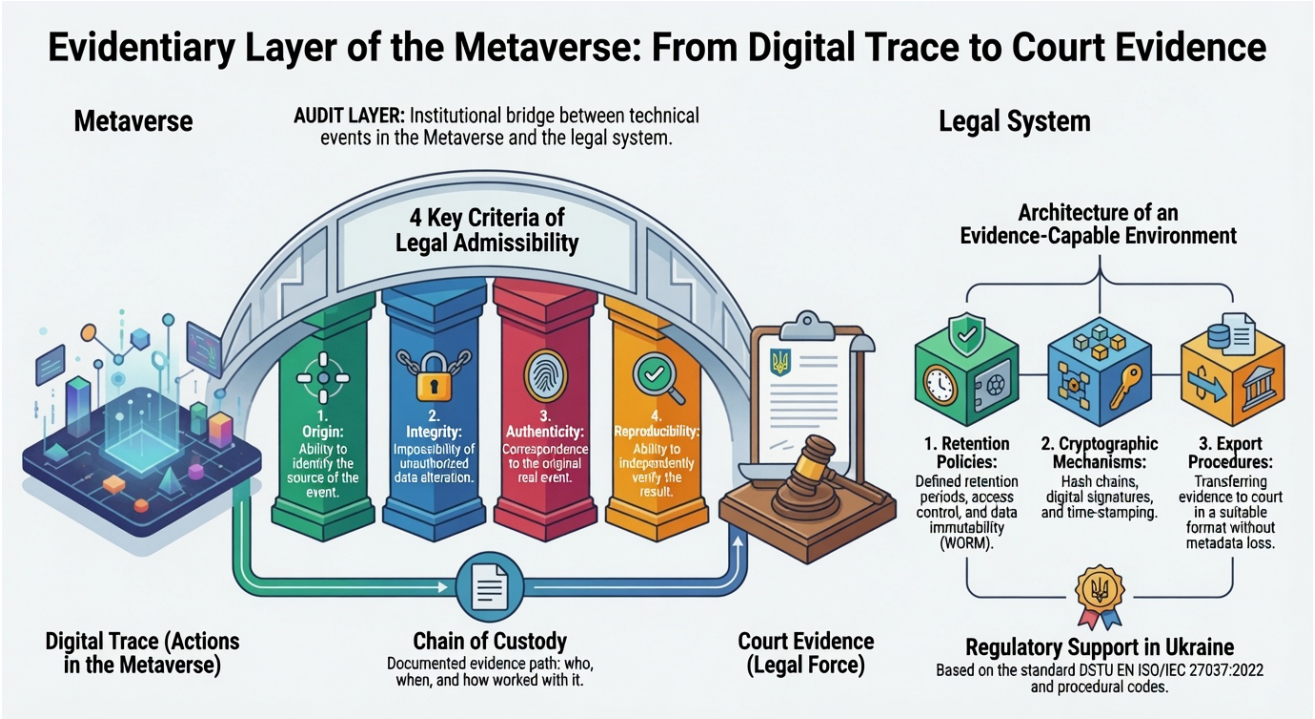


Figure 11. Metaverse: Proof Layer.

This is important for the study, because it allows us to substantiate that the audit layer is not a "technical appendix", but a procedural mechanism for implementing the requirement of a fair trial — in terms of adversarial, equality of the parties and verifiability of evidence (Figure 11).

In the plane of the Metaverse architecture, the audit layer must include at least three blocks of technical and legal guarantees.

The first is retention and immutability policies: defined terms, WORM storage modes for critical logs, access control by roles, logging administrative actions, time synchronisation.

The second is cryptographic confirmation mechanisms: hash chains, signing a proof package, time-stamping where relevant, as well as documenting algorithms and versions of the software environment that form artifacts.

The third is the procedures for exporting/transferring evidence in a format suitable for the court and the expert, preserving metadata and context (session ID, spatial coordinates, sensor parameters, "scene" version, change logs). It is these blocks, being "stitched" with the standard for handling digital evidence, that form the practical content of the chain of custody in the Metaverse environment.

A separate but increasingly significant dimension is the use of VR/3D reconstructions to recreate events and present evidence in pre-trial investigation and trial procedures. Here, the evidentiary problem is complicated by the fact that VR reconstruction is often not a "primary trace", but an analytical visualisation of data (a set of measurements, photos/videos, diagrams, readings), that is, in fact, the result of an expert transformation. Ukrainian research on 3D modelling in forensic science (in particular in expert reconstructions) demonstrates the practical value of spatial reproduction, but at the same time implies the need for strict requirements for the methodology, input data and verification of the result.

Legally, this means: VR representation must be accompanied by a description of data sources, construction methods, errors, as well as a counter-check procedure by the defence/opponent, otherwise there is a risk of turning into a "convincing illusion" without a proper evidentiary basis.

Thus, the audit layer is the procedural heart of the Metaverse digital jurisdiction, since it ensures the transformation of an event into evidence, and evidence into a legal fact suitable for recognition, appeal, and use in motivating a decision. Standardisation (DSTU EN ISO/IEC 27037:2022), the consolidation of electronic evidence in procedural codes, and the development of scientific and methodological approaches to admissibility form a regulatory basis, but practical implementation depends on whether the Metaverse is designed as an evidence-based environment. It is the evidentiary requirement that should be included in the Metaverse's "legal ontology" along with identity, data, content, and transactions: without it, platform accountability remains a declaration, and e-jurisdiction remains a theoretical construct.

1.4.8. Layer of sanctions and their application.

Sanctions in the Metaverse manifest themselves in various forms: technical restriction of access, blocking of accounts, removal of content, economic restrictions, "protocol" sanctions, as well as state enforcement (if there is a jurisdictional binding). In view of the above, the architecture of sanctions should be described as a system of procedures: trigger (violation of the rule/law); competent entity (operator/arbitration/court); evidentiary standard; proportionality; review/appeal. In the context of the autonomy of procedures and the use of AI systems in moderation and risk management, the requirements of risk-based governance and accountability, enshrined both in the NIST AI RMF (National Institute of Standards and Technology, 2023)[1] and in the EU regulation on harmonised rules on AI, are applicable. At the same time, the strategic European discourse on Web 4.0 and virtual worlds explicitly emphasises interoperability, security, and trust as prerequisites for the next technological transition.

1.4.9. Multi-Level Trust, Compliance, and Risk Management in the Metaverse.

Trust in the Metaverse is a backbone category because the user interacts not only with people but also with the platform, protocol, AI agents, and tokenised assets. In scientific approaches, it is advisable to distinguish: infrastructure trust (to protocols, networks, cryptography, identification), functional (to services and their stability), personalised (to avatars/participants and their reputation), normative (to rules, moderation mechanisms, dispute resolution procedures and enforcement of decisions). It is regulatory trust that is the contact between platform rules and public law: without procedures that ensure predictability and fairness, the Metaverse becomes a space of private power without proper accountability.

If we build a scientific and legal framework for the Metaverse, then the positions given in the previous paragraph describe "disparate technical slang words", and as a managed chain of trust: MetaGuard (who are you?) - CACMTM (can you trust the here and now?) - Privacy-Preserving AI/HE (can we process data without unnecessary risk?)

1 National Institute of Standards and Technology. (2023, January). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

- XAI/Fairness/Non-IID (are solutions reasonable, fair and reproducible?) - Edge/Reconfigurable/Neuromorphic (will it withstand latency and scale?) - DLT/IP-dApp (do we fix our rights and events in such a way that they are recognised?) - Green/Quantum-safe (whether the system is stable in energy and cryptographic horizon). It is this "bundle" that is best translated into regulatory requirements: from technical standards and policies to legal and functional definitions of risk and liability.

One of the main criteria of the Metaverse is trust and its provision at all possible levels. An interdisciplinary study has identified four levels of trust:

infrastructural (trust in protocols),
functional (trust in systems and services);
personalised (trust in avatars and users);
normative (trust in regulatory mechanisms).

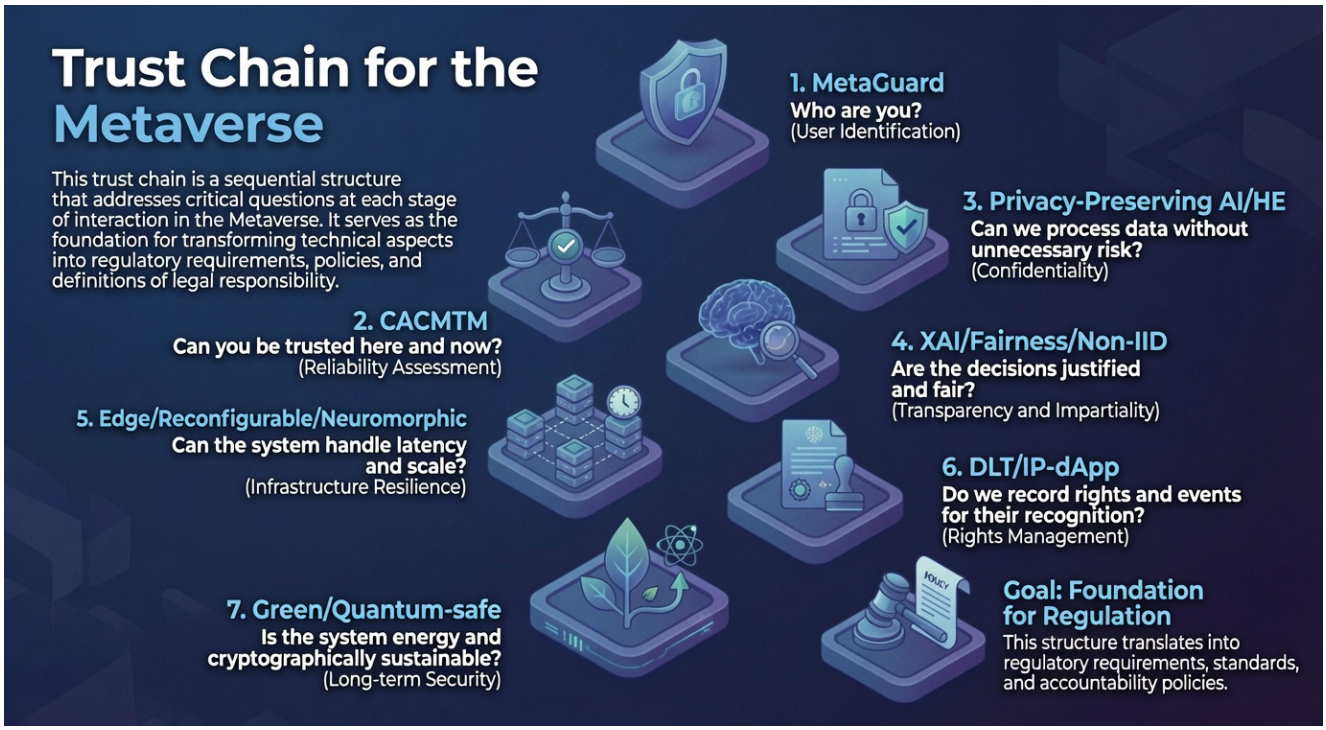


Figure 12. Metaverse: Levels of Infrastructure Trust.

Infrastructure trust (trust in protocols and institutions) is trust in the underlying structures, protocols, institutions, or technology platforms that ensure stability and predictability in the functioning of the system (Figure 12) (McKnight et al., 2002)[1]. A high level of institutional trust promotes organisational commitment, improves cooperation between companies and reduces uncertainty in business (Steinsbekk & Myskja, 2020)[2], improves the quality of public administration, fairness of services, reliability of technological solutions (Lewicka, 2020)[3].

1 McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

2 Steinsbekk, K., & Myskja, B. (2020). Personalized medicine, digital technology and trust: a Kantian account. *Medicine, Health Care, and Philosophy*, *23,* 577 - 587. https://doi.org/10.1007/s11019-020-09974-z

3 Lewicka, D. (2020). Employee institutional trust as an antecedent of diverse dimensions of organisational commitment. *Argumenta Oeconomica, 1*, 333–356. https://doi.org/10.15611/aoe.2020.1.13

Functional trust (trust in systems and services) - trust in specific functions, services or processes that perform certain tasks (Lucero et al., 2020)[1].

Personalised trust (trust in avatars and users) is trust formed in interactions between individuals, avatars or representatives of organisations (Wieselthier et al., 2012)[2] and includes interpersonal trust, role-based trust, as well as trust in specific participants or teams.

Regulatory trust (trust in regulatory mechanisms) - trust in rules, norms, ethical standards and regulatory mechanisms that determine the behaviour of system participants (Pohle et al., 2020)[3] ensures legitimacy, fairness and predictability in interactions, especially in the context of digitalisation and personalised medicine and is closely related to institutional trust, but focuses on rules and standards (Figure 13) (Siegrist & Bearth, 2021)[4].

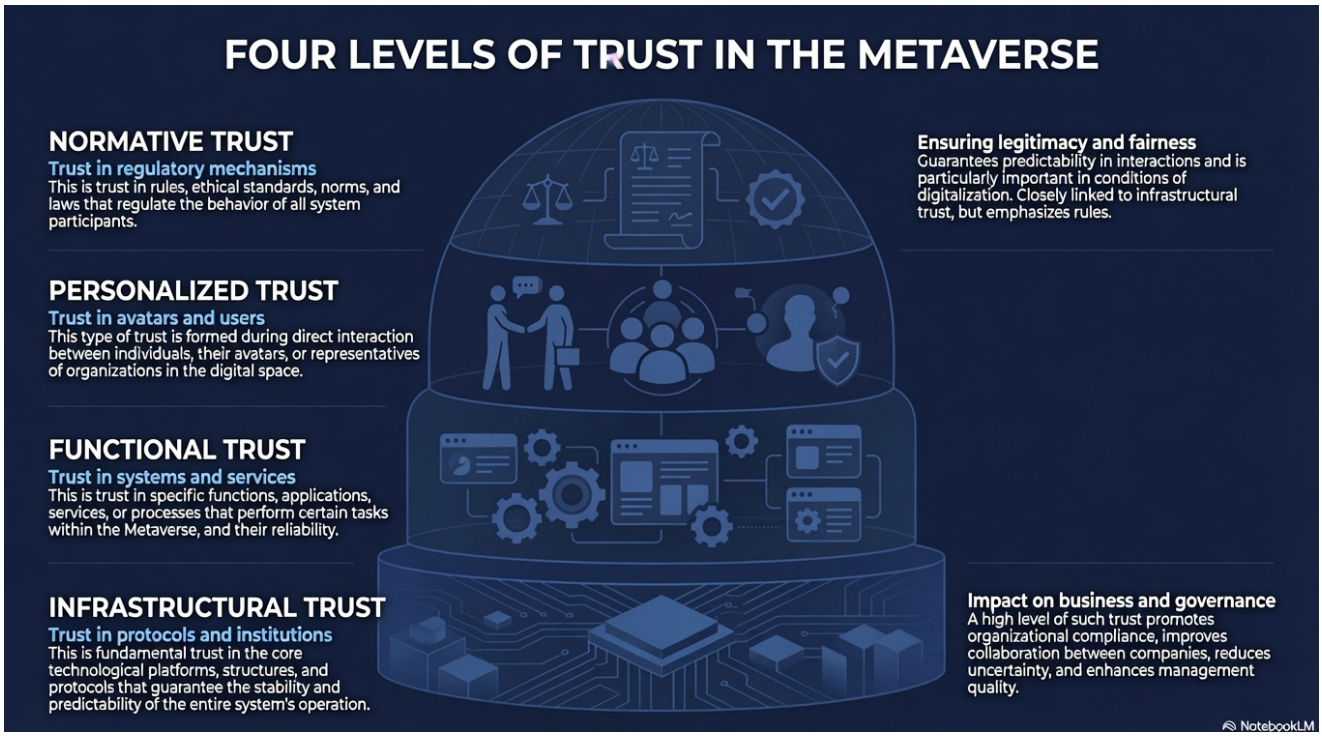


Figure 13. Metaverse: Levels of Regulatory Trust.

The interrelationship and dynamics of levels of trust: institutional and normative trust form the basis for functional and personalised trust. Trust develops progressively — from basic infrastructural trust towards more complex personalised and normative trust.

1 Lucero, J., Greene-Moton, E., Oetzel, J., Eder, M., Boursaw, B., & Wallerstein, N. (2020). Engage for equity: The role of trust and synergy in community-based participatory research. *Health Education & Behavior, 47*(3), 372–379. https://doi.org/10.1177/1090198120918838.

2 Wieselthier, E., Gelfand, M., Reitter, R., Laforge, H., Colston, M., Sweeney, B., Vaughn, M., Barley, E., Wilson, E., Von Numers, S., Jimenez, N., Raines, W., Lenoir, E., Al-Mansoor, F., & Fulmer, C. (2012). At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management, 38*(4), 1167–1230. https://doi.org/10.1177/0149206312439327.

3 Pohle, S., Niedlich, S., Kallfaß, A., & Bormann, I. (2020). A comprehensive view of trust in education: Conclusions from a systematic literature review. *Review of Education, 8*(1), 124–158. https://doi.org/10.1002/rev3.3239

4 Siegrist, M., & Bearth, A. (2021). The social amplification of risk framework: A normative perspective on trust? *Risk Analysis, 42*(7), 1381–1392. https://doi.org/10.1111/risa.13757.

1.4.10. The genesis of the legal regulation of the Metaverse.

Historically, our civilisation has gone through three communication epochs — verbal, when information in society was transmitted only orally; verbal-symbolic, when information was transmitted both orally and with the help of special symbols — letters, words, actions, events; verbal and written, during which printed literature appeared. Today, humanity has entered the fourth era — the era of dominance of electronic communication, where information and communication technologies are integrated with previous forms of communication.

This era also went through a transformation from archaic computers to universal technologies. The Metaverse is becoming not only a progressive era of communication, but also a new scientific and technical centre for the development of society, an accumulator and constructor of modern technologies, a generator of new flexibility, a tool that helps people survive. It becomes an independent environment that functions in parallel with the physical world and laws, which requires some rethinking in today's society (Shaoying et al., 2022)[1].

The future Metaverse will be a large open scalable system. This system is being created simultaneously, encompassing cyberspace, hardware terminals, various manufacturers and users, providing a wide range of application scenarios in virtual and augmented reality (AR/VR environments), demonstrating the ultimate form of a super-ecosystem. However, without proper legal regulation, the territory of "virtual freedom" can turn into a destructive tool, requiring regulation of social relations in the Metaverse (Pengfei, 2022)[2].

Today, there are several different Metaverses: Horizon Worlds, Ceek city, Baidu Xi Rang, Metaverse Facebook, Decentraland (Ethereum), Metaverse Emirates, Advanced Virtual World, Qualcomm Nvidia Omniverse using AI, AR/VR, holograms, XR platforms, distribution registers, neural networks, quantum technologies, and other technical solutions.

Obviously, the regulation of legal rights in the Metaverse is the boundary between electronic gaming software and application products, and their legal regulation is fragmented and situational, with the application of existing analog laws and regulations, such as codes, regulations, and standards.

There is an approach to conducting "experimental legal regimes", known in the world as "regulatory sandboxes" (SandBox), within the framework of which the government determines special legal regulation for a certain period in certain areas for the development of the AR/VR environment.

The practice of using the Metaverse already has several precedents for the application of certain provisions to resolve legal uncertainty in the virtual environment, such as the establishment of ownership of virtual intangible assets, the purchase/sale of virtual intangible assets, liability for the misappropriation of virtual assets with signs of various types of discrimination and moral violence, the spread of ideologies of racism and fascism, etc. At the same time, there are more and more types of torts that have a

---

1Shaoying, P., Pengzhi, C., Xinru, F., Lifu, Q., Junhui, H., & Liwen, J. (2022). Ten conjectures: Interpretation of the development trend of the most comprehensive metaverse. *IT Times*. https://m.jiemian.com/article/7078158.html.

2 Pengfei, Z. (2022). If the metaverse is the future then what is the future of the metaverse? *Xinhuanet*. http://www.xinhuanet.com/techpro/20220120/264c62d021974eee81d70c35083ef91a/c.html

nature exclusively in the Metaverse and should be regulated exclusively within the Metaverse.

The problem of legal regulation of the use of identification (personal) data, which will become the basis for the creation and functioning of virtual avatars or electronic humanoids in the Metaverse, is taking on a new perspective.

Given the urgency of the problem, there is a need to create a single model of digital jurisdiction, on the basis of which the legislative framework for the Metaverse will be developed.

Currently, this approach has no analogues, and the proposed Metaverse Model of Digital Jurisdiction should become the basis not only for scientific discussions, but also for legal research in order to create primary model legislative acts that should ensure the legal regulation of social relations in the Metaverse, as well as initiate the digital transformation of analog legislative acts.

1.4.11. Formation of the concept of "information society".

The late 1990s and early 2000s were marked by the development of information and communication technologies related to the dissemination of information via the Internet. At that time, the environment of electronic resources was static websites designed to read and view — Web 1.0 technology. These information resources did not contain interactive elements, multimedia, and did not have functions that allowed users to communicate online, exchange files, etc. The website creation tool was a set of HTML markup language tags that served as a design. In addition, the internet connection speed was insufficient to transfer images and videos.

At the same time, many scientists saw in this technology prospects not only for application in broad fields of science and technology, but also for the formation of new social relations different from the existing ones. Scientists hoped that Web 1.0 and the Internet would allow society to create a new environment, free from state domination or not burdened by excessive legal requirements. authored by D. Barlow, and "Code and Other Laws of Cyberspace" by researcher L. Lessig. In the Declaration, the author presented cyberspace as a space of such power that is necessary to establish freedom. In fact, D. Barlow (1996)[1] stated that cyberspace — is a liberal virtual extraterritorial enclave that is not subject to any state jurisdiction and is intended for people free from any privileges and discrimination, which completely denies state interference in cyberspace.

Also, L. Lessig (1999)[2] determined that cyberspace is inevitable but unregulated, and society in the real world is governed by four main regulators: law, social norms, market relations, and "architecture/code" (technological capabilities). No nation can live without it, but no nation can control behaviour in cyberspace. Cyberspace — is a place where people are free from real control.

In our opinion, in accordance with the technological capabilities of the time and the state of social relations, L. Lessig considered its architecture, technical components or capabilities, or "code" to be the key regulator of cyberspace. It is the code that determines

1 Barlow, J. P. (1996). Declaration of the independence of cyberspace. *Electronic Frontier Foundation*. https://www.eff.org/cyberspace-independence

2 Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic Books.

the order of use of cyberspace, just as social relations in real space are subject to public administration. L. Lessig argues that in a fundamental sense, the code of cyberspace is its Constitution. The Code defines the conditions under which people access cyberspace and establishes rules that control their behaviour. The Code forms its own sovereignty, which is an alternative to real physical life.

In his work, L. Lessig (1998)[1] was the first to draw attention to the need for laws that would simultaneously ensure regulation in cyberspace and minimise restrictions on human rights and freedoms. L. Lessig offers several ways to deal with the "bleak" future: open source and the development of legislation (Viseu, 2001).[2] According to L. Lessig, open source should act as a kind of constitutional control, guaranteeing that all citizens can "read" and influence the "created" environment. Legislative measures are to adapt the Constitution (USA) to the conditions of cyberspace to ensure that modern values are protected and preserved in cyberspace.

Today, this approach can be called an attempt at "soft" or democratic regulation of cyberspace, which is mainly based on the creation of a legal framework for the use of certain technologies and almost does not provide for legal regulation of social relations.

At that time, the development of state legislation regulating cyberspace took place in two main directions: amendments and additions to the Criminal Codes and law-making through the development of a number of separate legislative acts.

The first direction was chosen by countries such as Canada, Estonia, Germany, Sweden, Finland, Austria, Italy, Latvia, the Netherlands, Spain, Poland and Ukraine. For example, Ukraine has introduced a separate section "Criminal offences in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks" in Articles 361 — 363 and 363[1] of the Criminal Code.

Regarding the creation of separate legislation, the following countries should be noted. Thus, in 2000, the Republic of India adopted the India, Information Technology Act, 2000, which provides legal regulation in the field of information and communication technologies and electronic signature technologies. This Law is interesting for the introduction of a special Cyber Appeals Tribunal to consider offences committed using modern cyber technologies. In addition, this Law introduces the classification of a number of crimes, including computer distribution of child pornography, electronic fraud and cyberterrorism, which involves the use of state coercion in the form of fines or restriction of liberty (Articles 66, 66A-66E, 67, 67A-C, 71-79).

The U.S. has enacted regulations to control the distribution of unwanted pornography and marketing (CAN-SPAM Act, 2003)[3], regarding fraud and related activities related to means of access (18 U.S.C. § 1029, 2015)[4],regarding fraud and related activities in the computer field (18 U.S.C. § 1030, 2020)[5], regarding fraud and related

1 Lessig, L. (1998). The laws of cyberspace. *Taiwan Net '98 Conference*. https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf

2 Viseu, A. (2001). Code and other laws of cyberspace (review of the book *Code and other laws of cyberspace*, by L. Lessig). *Canadian Journal of Communication, 26*(1), 179–180.

3 Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), 15 U.S.C. §§ 7701–7713 (2003).

4 18 U.S.C. § 1029 (2015).

5 18 U.S.C. § 1030 (2020).

activities in the field of e-mail (18 U.S.C. § 1037, 2003)[1], regarding the interception of telegraph, telephone and electronic communications, as well as oral communications (18 U.S.C. §§ 2510–2523, 2022)[2] and regarding access to stored wired and electronic communications and transaction records (18 U.S.C. §§ 2701–2713, 2018)[3].

During the same period, other countries enacted relevant laws: the Israeli Computer Law (Computer Law, 5755–1995)[4], the British Computer Misuse Act (1990)[5] and the French Act Relating to Data Processing, Files and Freedoms (1978)[6].

As you can see, society and states reacted differently to the emergence of Web 1.0 information and communication technologies. On the one hand, we have the position of forming liberal approaches to "soft" regulation of cyberspace, on the other hand, the state, as a regulator of social relations, establishes or sanctions generally binding rules that in a sense restrict the rights and freedoms of citizens, but these rules are provided by measures of state influence, including state coercion (Figure 14).

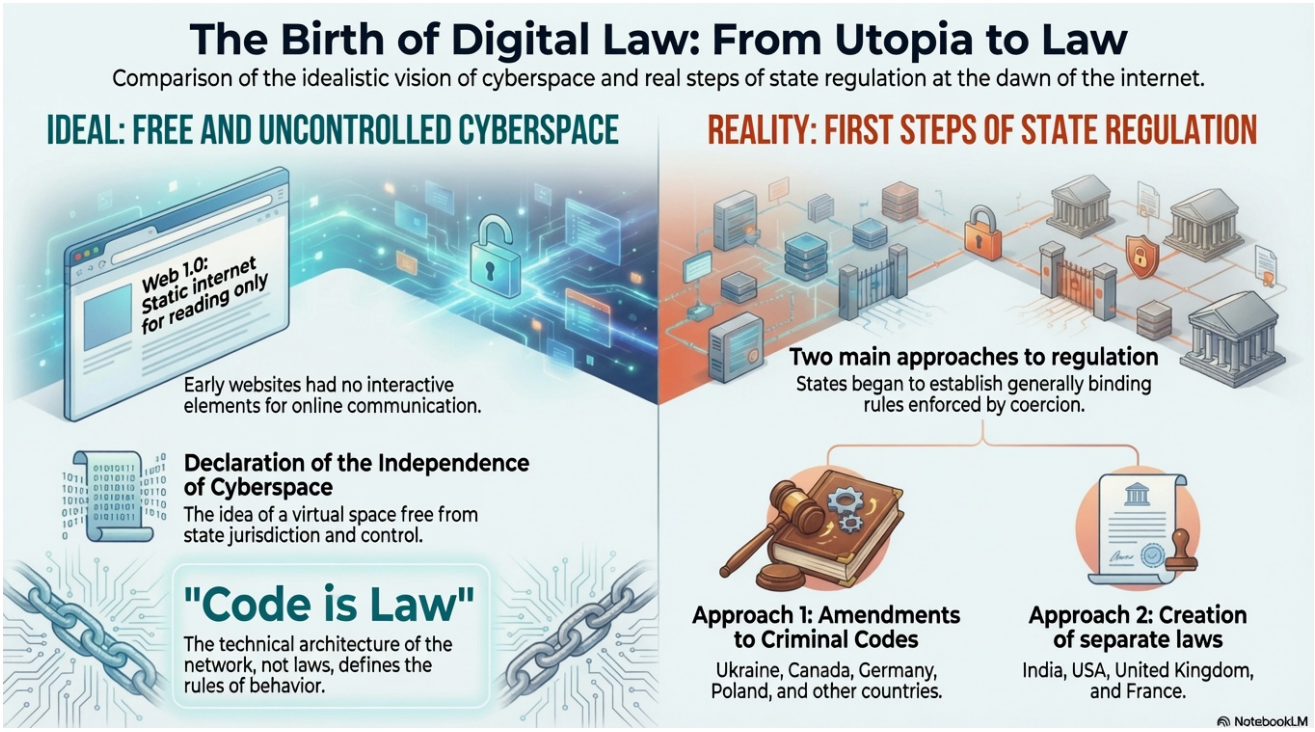


Figure 14. Metaverse: the birth of law for digital environments.

If Web 1.0 appears as the starting phase of digital communication and the "primary" cyberspace, in which scientific thought debatably outlined the boundaries of state jurisdiction, then the Metaverse is methodologically correct to comprehend as the next stage of the complexity of the information society: from static web resources to interactive platforms and further to persistent immersion environments, where the interaction of people, data, and things takes on the character of an almost continuous "digital presence".

1 18 U.S.C. § 1037 (2003)
2 18 U.S.C. §§ 2510–2523 (2022)
3 18 U.S.C. §§ 2701–2713 (2018).
4 Computer Law, 5755–1995 (Israel).
5 Computer Misuse Act 1990 (UK)
6 Act №. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Fr.). https://www.cnil.fr/en/act-no-78-17-6-january-1978-data-processing-files-and-liberties-amended

In the legal sense, this means a change in the subject matter of information law: from the regulation of "transmission and access to information" to the regulation of modes of presence, identity, behavioural interaction and high sensitivity data generated as a condition for the functioning of the environment. In view of the above, the Metaverse is not "another application of the Internet", but appears as an infrastructural form of organising digital experience, within which "architecture/code" again comes to the fore as a regulator — but in a much more complex technological and socio-legal context than in the Web 1.0 era.

In modern scientific and technical discourse, the Metaverse is usually defined as a network of interconnected virtual spaces that support real-time interaction through avatars, 3D objects, and digital services, integrating XR (VR/AR/MR), artificial intelligence, cloud and edge computing, high-speed communication networks, and sometimes distributed ledgers (Cali et al., 2022)[1]. For information law, it is advisable to decompose this definition into legally relevant properties:

1) immersion as an "embodied" participation that increases the value of biometric and spatial data;

2) persistence as a continuity of the environment, which determines new modes of data storage and digital footprint;

3) social presence as a plurality of subjects and collective actions, which actualises the rules of moderation, due process and responsibility;

4) data-centricity as a systematic production of data streams about behaviour, movement, voice, biometrics and context.

It is this data-centricity that makes the Metaverse a direct continuation of the information society, but at the same time it exacerbates the issue of digital law as a law of "high data density", where privacy, security, and evidence cease to be "applied" topics and become the core of the legitimacy of the environment.

In the plane of Industry 4.0, it is advisable to consider the Metaverse as a universal layer of visualisation, simulation and coordination of cyber-physical processes, within which digital twins (equipment, production lines, logistics, infrastructure) are presented in the form of interactive models and scenarios. Practical potential is manifested in digital prototyping, remote maintenance, and personnel training through simulations of risky operations, the collaboration of engineering teams in a 3D environment, the reproduction of supply chains as an "operational map", as well as in new skill certification formats. In such cases, the Metaverse is not an "entertainment", but a space for managing complexity, where data accuracy and trust become legally relevant for occupational safety, man-made safety, product quality, auditing, compliance, and responsibility (Chen et al., 2024). [2]There is a direct analogy with information law: as in classical information systems, the law determines the mode of access, processing, storage and protection of information, for example, in the Metaverse, the law must define the mode of "digital production

1 Cali, U., Kuzlu, M., Karaarslan, E., & Jovanovic, V. (2022). Opportunities and challenges in metaverse for Industry 4.0 and beyond applications. In *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)* (pp. 1–6). IEEE. https://doi.org/10.1109/iGETblockchain56591.2022.10087104

2 Chen, H., Duan, H., Abdallah, M., Zhu, Y., Wen, Y., El Saddik, A., & Cai, W. (2024). Web3 metaverse: State-of-the-art and vision. *ACM Transactions on Multimedia Computing, Communications, and Applications, 20*(4), Article 101, 1–42. https://doi.org/10.1145/3630258

management" — with requirements for the reliability of the digital twin, the admissibility of data for audits and investigations, and the procedural suitability of event logs.

Beyond manufacturing, Metaverse opens up a wide range of applications in education, healthcare, retail, culture, public services, and social communication. At the same time, the social effect is not reduced to the emergence of "new services", since immersion changes the form of human participation in the digital environment — from "viewing" information to behavioural interaction with the environment. This means that the legal categories formed for Web 1.0 (content, access, copyright, general cybersecurity rules) in the Metaverse are complemented by the categories of "presence", "behavioural footprint", "data corporeality" (biometric and spatial parameters), "avatar identity" and "contextual privacy". In terms of information law, this can be presented as a shift from the regulation of "information messages" to the regulation of modes of information interaction, where the very architecture of interfaces and the XR sensory circuit become a source of data and at the same time a mechanism for influencing behaviour.

A separate dimension is the Metaverse's connection to the Web3 paradigm, where the emphasis is on asset tokenisation, smart contracts, decentralised accounting mechanisms, and digital identity tools. Such approaches describe Metaverse as an environment in which identity can be implemented through mechanisms such as decentralised identifiers (DIDs), digital objects, and access rights — through tokens (including NFTs as uniqueness/ownership tokens or usage rights), reputation or "irrefutable attributes" — through non-transferable tokens (in some concepts, "soulbound") (Wang et al., 2022)[1]. Legally, this unfolds into the legal nature of virtual assets, the validity and enforceability of the terms of a smart contract, as well as the distinction between "technical possession of the key" and "legal possession of the right" (Choi et al., 2022)[2]. At the same time, even with Web3 tools, there is still a systemic risk: technical decentralisation does not guarantee social or economic decentralisation, and therefore requires legal safeguards against the monopolisation of access rules, interoperability standards, and moderation models — in the logic of information law, this corresponds to the topics of platform power, rules for access to digital resources, and publicly significant private regimes (Chang et al., 2023)[3].

The most conceptually loaded challenge block for the Metaverse is security, privacy, and trust, as immersion systems work with more sensitive data than classic web platforms: geolocation, motion tracking, voice and visual patterns, behavioural reactions, and sometimes biometrics, and environmental parameters. This data is collected continuously and is often functionally necessary (realism, synchronisation, personalisation), which is why the risk of invasion of privacy becomes non-episodic, and of a structural nature. In the field of information law, this means the need to rethink the classic tools of consent, data minimisation, target restriction and access modes, because the "default collection"

1 Wang, Y., Su, Z., Zhang, N., et al. (2022, October 10). A survey on metaverse: Fundamentals, security, and privacy. *TechRxiv*. https://doi.org/10.36227/techrxiv.19255058.v3

2 Choi, M., El Azzaoui, A., Singh, S. K., Salim, M. M., Jeremiah, S. R., & Park, J. H. (2022). The future of metaverse: Security issues, requirements, and solutions. *Journal of Big Data, 9*, Article 60. https://doi.org/10.1186/s40537-022-00683-3

3 Chang, V., Strittmatter, S., Jesus, V., Golightly, L., Ni, P., & Hall, K. (2023). Exploring risks in the metaverse in an immersive digital economy. In *Proceedings of the 5th International Conference on Finance, Economics, Management and IT Business (FEMIB)* (pp. 107–113). SciTePress. https://doi.org/10.5220/0011990900003494

becomes technically built-in. At the same time, cybersecurity threats are growing: account compromise, avatar spoofing, attacks on software supply chains, vulnerabilities in XR devices, fraud in virtual asset economies, manipulation through social engineering in the "environment of presence". So, legal compliance here is a transition to security-by-design and privacy-by-design modes as mandatory elements of the provider's proper behaviour, rather than voluntary "best practices".

An equally significant systemic challenge is interoperability (interoperability), i.e. the ability of different platforms and services to exchange identities, assets, access attributes, and evidence. For digital law, this issue has two sides: technical (standards of protocols, formats, cryptographic mechanisms, security policies) and legal (recognition of rights, ownership/use regimes, liability and evidence of "events"). In terms of information law, interoperability is an analogue of "compatibility of legal regimes" for information systems: just as in the field of electronic document management, the mutual acceptability of formats and trust services is critical, so in the Metaverse the mutual acceptance of identity, access attributes and event logs becomes critical. In practice, this means that a dispute or incident can span multiple jurisdictions and multiple "architectures", and thus the classical model of territorial law faces the need for procedural mechanisms of cross-border recognition, digital proof, standardisation of logs, retention chains, and clear rules regarding the roles of providers, developers, administrators, and users (Uddin et al., 2023; Ramírez-Herrero et al., 2023)[1, 2].

It is here that the logic about "code" as the constitution of cyberspace and the relationship between "soft" regulation and state coercion takes on a new depth. In the Metaverse, "code" does define opportunities and prohibitions, but now it interacts with platform governance, economic incentives, algorithmic systems (moderation, recommendations, anti-fraud), as well as with government requirements for data protection, cybersecurity, crime prevention, and human rights protection (Johri et al., 2024)[3].

Therefore, the regulatory model for the Metaverse reasonably moves towards a multi-level structure: architectural and protocol restrictions (security-by-design, privacy-by-design), contractual rules of platforms and standards, industry norms and codes of ethics, national and international law (data, security, consumer protection, childhood, non-discrimination), procedural guarantees of due process for decisions affecting user rights and access. In the terminology of information law, this approach can be described as a transition from "information rationing" to the regulation of the digital environment — where subordination and legitimacy must be ensured procedurally, evidentiarily, and technologically[4].

---

1 Uddin, M., Manickam, S., Ullah, H., Obaidat, M. S., & Dandoush, A. (2023). Unveiling the metaverse: Exploring emerging trends, multifaceted perspectives, and future challenges. *IEEE Access, 11*, 87087–87103. https://doi.org/10.1109/ACCESS.2023.3281303.

2 Ramírez-Herrero, V., Ortiz-de-Urbina-Criado, M., & Medina-Merodio, J.-A. (2023). The Metaverse Revolution: Critical Analysis of Its Lights and Shadows. *ESIC Market, 54*(3), e334. https://doi.org/10.7200/esicm.54.334

3 Johri, A., Sayal, A., N, C., Jha, J., Aggarwal, N., Pawar, D., Gupta, V., & Gupta, A. (2024). Crafting the techno-functional blocks for metaverse: A review and research agenda. *International Journal of Information Management Data Insights, 4*(1), 100213. https://doi.org/10.1016/j.jjimei.2024.100213

4 Pu, Q., & Xiang, W. (2022). The metaverse and its influence and transformation on human society. *Metaverse, 3*(1). https://doi.org/10.54517/met.v3i1.179.

It is worth emphasising that the "opportunities" of the Metaverse for Industry 4.0 and related areas can be legally feasible only if the trust architecture — digital identity, access, logging, auditing, interoperability — is normatively and procedurally enforced. In other words, information law here must fulfil its classic role of "the law of conditions": to determine under which legal regimes data become evidence, access — lawful, moderation — procedurally fair, and transactions are executable and accountable. It is this formulation of the question, in our opinion, that allows us to avoid reducing the Metaverse to a technical trend and turn it into a subject of systemic legal analysis in the coordinates of digital law and digital jurisdiction[1].

1.4.12. Methodology of Legal Regulation of Web 2.0

Since 2004, the term "Web 2.0" has become widespread as characterising the next stage in the development of information and communication technologies. In the future, it will often be used together with the term "scientific and technological revolution 4.0", as they describe significant changes in society that are taking place as a result of digitalisation.

The term Web 2.0 refers to a comprehensive combination of technologies such as high-speed internet protocols, fifth-generation (5G) mobile communications, and numerous standards for wireless networks, interactive websites, resources, and platforms. The main difference between Web 2.0 and Web 1.0 is that content is created and produced by users who are both consumers of content and do not own technical resources. At the same time, the emergence of Web 2.0 as an environment free from state domination and unencumbered by excessive legislation is characterised by the emergence of the Darknet network, cybercrime, malware, anonymous hackers, cryptocurrency, pirated content, destructive information, etc.

At the same time, "electronic" legislation was actively developing — national and international; in the field of information, criminal, civil, administrative law; intellectual property rights; as well as technical regulation of information and communication technologies through regulations, rules, certification, etc. (Figure 15). For example, the regulation of the use of Internet of Things devices is carried out simultaneously with the introduction of technical and legal regulation (Kostenko, 2021b)[2], and the management of AI use is being shaped by many countries in accordance with the adopted AI Development Strategies (Zhang et al., 2021; Zhang et al., 2022)[3, 4].

---

1 Wider, W., Jiang, L., Lin, J., Fauzi, M. A., Li, J., & Chan, C. K. (2023). Metaverse chronicles: A bibliometric analysis of its evolving landscape. *International Journal of Human–Computer Interaction*. https://doi.org/10.1080/10447318.2023.2227825

2 Kostenko, O. (2021b). Identyfikatsiia IoT. *Juris Europensis Scientia, 1*, 77–83. https://doi.org/10.32837/chern.v0i1.177

3 Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J. C., Sellitto, M., Shoham, Y., Clark, J., & Perrault, R. (2021). *Artificial Intelligence Index Report 2021*. Stanford Institute for Human-Centered Artificial Intelligence. https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Master.pdf

4 Zhang, D., Maslej, N., Brynjolfsson, E., Etchemendy, J., Lyons, T., Manyika, J., Ngo, H., Niebles, J. C., Sellitto, M., Sakhaee, E., Shoham, Y., Clark, J., & Perrault, R. (2022). *Artificial Intelligence Index Report 2022*. Stanford University, Stanford Institute for Human-Centered Artificial Intelligence. https://aiindex.stanford.edu/report/

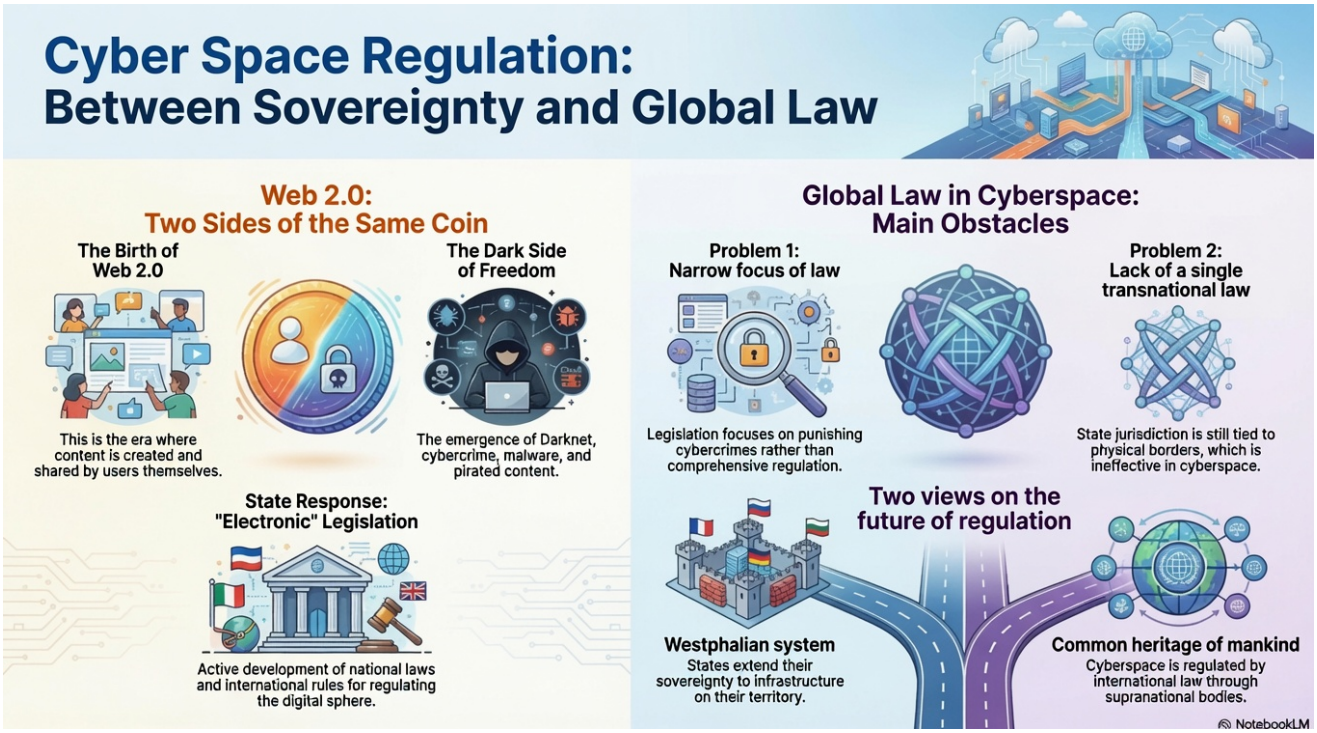


Figure 15. Regulation of cyberspace.

A significant number of international documents on the information society were developed and adopted on the initiative and participation of non-governmental organisations. When solving infrastructure issues of the Internet organisation, the position of a sovereign state has not always been and is the main priority. Effective regulators of the global information society have become instruments of "soft" international law, which, although not binding, respond extremely quickly to new challenges and reflect interests of all interested subjects. However, non-binding rules have significant regulatory and persuasive value. That is, technological innovations should be taken into account in the development of relevant regulations (Kyryliuk, 2015)[1]. For example, Ukraine has been in no hurry to develop modern legislation in the field of information technology for some time and has been rather slow to digitise both public authorities and recodify existing legislation. However, recently the Verkhovna Rada of Ukraine has developed and adopted a number of modern regulatory legal acts, such as the Laws of Ukraine "On the Protection of Information in the Field of Information Protection". Information and Communication Systems" (Ukraine, 1994)[2], "On Electronic Trust Services" (Ukraine, 2017)[3], "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (Ukraine, 2017)[4], "On Critical Infrastructure" (Ukraine, 2022a)[5], "On Virtual Assets" (Ukraine, 2022a)[6] and

1 Kyryliuk, O. (2015). Miake pravo yak normatyvna osnova hlobalnoho informatsiinoho suspilstva. *Actual Problems of International Relations, 125*(Part 1), 106–117. http://apir.iir.edu.ua/index.php/apmv/article/view/2664/2368.

2 Ukraine. (1994, July 5). Law of Ukraine on protection of information in information and communication systems (№. 80/94-BP). https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

3 Ukraine. (2017a, October 5). *Law of Ukraine on electronic trust services* (№. 2155-VIII). https://zakon.rada.gov.ua/laws/show/2155-19

4 Ukraine. (2017b, October 5). *Law of Ukraine on the basic principles of ensuring cyber security of Ukraine* (№2163-VIII). https://zakon.rada.gov.ua/laws/show/2163-19

5 Ukraine. (2021, November 16). *Law of Ukraine on critical infrastructure* (№. 1882-IX). https://zakon.rada.gov.ua/laws/show/1882-20

6 Ukraine. (2022, February 17). Law of Ukraine on virtual assets (№. 2074-IX). https://zakon.rada.gov.ua/laws/show/2074-20

the Order of the Cabinet of Ministers of Ukraine "On Approval of the Concept for the Development of Artificial Intelligence in Ukraine" (Ukraine, 2022b)[1]. In 2019, the Ministry of Digital Transformation of Ukraine was established, whose task is to digitise public authorities and public administration mechanisms. The judicial system of Ukraine is introducing such digital mechanisms as electronic justice and electronic registers.

Modern global legal regulation of cyberspace has significant achievements, but they are offset by two problems:

1. the focus of law on the formation of legal responsibility for cybercrimes, as special types of crimes committed using digital tools in the national and cross-border information and communication environment (Riek & Böhme, 2018)[2];

2. the absence of a single transnational law that would ensure social relations not only at the national, but also at the transnational level (Razmetaeva et al., 2021)[3], in which the postulate that jurisdiction should not be tied to a certain territory or borders gradually acquires public importance, and the technical possibilities of regulating cyberspace are limited both objectively and subjectively (Vartanian, 2000)[4].

Today, scientific discussions are conducted around the issue of the territoriality of cyberspace as a whole and its individual elements. In the form in which cyberspace functions now, its connection with borders, national and international law is still quite clear and proportionally dependent. There is a real possibility of a technical division of cyber incidents into jurisdictions of national and international law. And the law performs within these limits the vast majority of its functions, namely: economic, political, ideological, cultural-educational, regulatory, educational, protective and preventive, taking into account national characteristics.

The state extends its sovereignty to the physical level, i.e. to the infrastructure located on its territory. The state exercises sovereign power on its territory. The state can also protect its control over cyberspace and cybercrime occurring on its territory. In addition, the state is obliged to protect its sovereignty, including information sovereignty, which passes through its infrastructure, takes place or ends in its territory, or is transmitted through national technical nodes. This indicates that under current international law, the rules of territorial restrictions may apply to cyberspace in its current form. The difference between the physical world and cyberspace is that power in the physical world is organised and operates in certain territories, while in cyberspace power is direct, not fragmented or identical to the boundaries of cyberspace. People can transfer certain activities and activities into cyberspace, they can nominally/virtually populate cyberspace, but they can never remove themselves from the real world in real life. This means that cyberspace and its organisation cannot be independent of states and, therefore,

1 Ukraine. (2020). *Order of the Cabinet of Ministers of Ukraine on the approval of the concept of the development of artificial intelligence in Ukraine*. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80

2 Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity, 4*(1), tyy004. https://doi.org/10.1093/cybsec/tyy004

3 Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021). Jurisdictional issues in the digital age. *Ius Humani. Law Journal, 10*(1), 167–183. https://doi.org/10.31207/ih.v10i1.240.

4 Vartanian, T. (2000). Whose laws rule the Internet? A U.S. perspective on the law of jurisdiction in cyberspace. *International Law FORUM du droit international, 2*(3), 196–201. https://doi.org/10.1163/157180400322765009.

cyberspace cannot be sovereign, since power in cyberspace is indirectly exercised by states (Tsagourias, 2018)[1].

That is why many researchers are inclined to the projection of the Westphalian system on the "state structure" of cyberspace, because thanks to it, the concept of a sovereign state and its main features, the principles of equality in relations in the system of international law were formed, the institution of international guarantees, equality of states, the concept of sovereignty, and the solution of international problems by peaceful means were introduced (Demchak & Dombrowski, 2014)[2]. At the same time, analysing the current legislation, the concept of the Common Heritage of Humanity (SSL) is proposed, according to which the regulation of cyberspace should be carried out by international law (Segura-Serrano, 2006)[3]. The concept of the SSL implies the need to establish international Internet governance bodies, reach consensus on intellectual property and protection of rights, privacy issues, the use of force and self-defence in cyberspace.

The future of e-justice in cyberspace is a separate issue. Currently, there are many examples of successful decisions on local electronic court systems, for example, in the Federative Republic of Brazil, the People's Republic of China and other countries.

Some researchers (Keddell, 2019; Razmetaeva & Razmetaev, 2021)[4,5] rightly emphasise certain risks of e-justice, which consist in the difficulties of synchronous integration of the main electronic tools into national justice systems, as well as the possible bias of e-justice algorithms. Moreover, this can be both a deliberate bias laid down by the developers, and an unintentional bias that duplicates the biases formed in analog justice.

Of course, there are scientists who share L. Lessig's theory of cyberspace law, based exclusively on cyberspace code, and propose to use the CyberLaw protocol (Gervais, 2004)[6]. CyberLaw is a network protocol redesigned in accordance with the rules of existing legal systems, which is transformed into an alternative form of indirect "invisible" legislation. That is, some of the legal risks in cyberspace are blocked and corrected by the CyberLaw protocol at the stage of their creation.

1.4.13. Metaverse Structure Based on Web 3.0 Technologies

Today, we are observers, participants and users of the latest information technologies, which have already received the common name Web 3.0. Web 3.0 technologies — are information and communication decentralised electronic virtual eco-networks that function on the basis of blockchain, electronic neural networks, machine

1 Tsagourias, N. (2018, July 13). *Law, borders and the territorialisation of cyberspace*. SSRN. https://doi.org/10.2139/ssrn.3213511

[2](Demchak & Dombrowski, 2014)3 Demchak, C. C., & Dombrowski, P. (2014). Cyber Westphalia: Asserting state prerogatives in cyberspace. *Georgetown Journal of International Affairs, 15*(2), 29–38

3 Segura-Serrano, A. (2006). Internet regulation and the role of international law. In A. von Bogdandy & R. Wolfrum (Eds.), *Max Planck Yearbook of United Nations Law*, *10*, 191–272.

4 Keddell, E. (2019). Algorithmic justice in child protection: Statistical fairness, social justice and the implications for practice. *Social Sciences, 8*(10), 281. https://doi.org/10.3390/socsci810028

5 Razmetaeva, Y., & Razmetaev, S. (2021). Justice in the digital age: Technological solutions, hidden threats and enticing opportunities. *Access to Justice in Eastern Europe, 4*(2), 104–117. https://doi.org/10.33327/AJEE-18-4.2-a00006

6 Gervais, N. (2004). From laws for cyberspace to cyber laws (literally): Integration of legal norms into Internet protocols and law for closed digital management communities. *SCRIPT-ed, 1*(2), 259–271. https://doi.org/10.2966/scrip.010204.259.

learning, artificial intelligence, Internet of Things, cryptocurrencies, virtual and augmented reality, and constant availability. According to research, the term "Metaverse" is currently the most popular, has many interpretations and is used to describe digitisation processes in almost all areas of human life (Özkahveci et al., 2022)[1].

Web 3.0 is the launching pad for the start of the scientific and technological revolution 5.0 and the next stage of human development — electronic humanoids and the Metaverse. There is no one-size-fits-all definition of the Metaverse.

The Metaverse characterises an infinite number of virtual worlds in which and between physical and digital subjects and objects endowed with certain properties: rights, duties and responsibilities socially interact. A key element of the Decentralised World is the identification of physical and digital entities and objects. Identity is a pass to the Metaverse.

Taking into account the main features of the post-industrial society and the trends of the transition period to it from the industrial one, it can be predicted that the Metaverse will go through the following three phases of development (Figure 16):

the first phase — the Metaverse shell (the basic layer of software and engineering), the entities and objects are completely dependent on the developers and owners of the shell;

the second phase — the Metaverse shell, entities and objects are owned by developers and partially owned by owners/users;

the third phase — Metaverse does not belong to specific developers, the management of subjects and objects is carried out either by the owner (hardware bioidentification) or autonomously (subjects and objects are endowed with functionality and rights inherent in the owner).

Only individuals will be considered Metaverse entities, and the category of objects will include legal entities, avatars, electronic personalities, virtual digital works of AAI and ASI, digital humanoids, intangible electronic assets of all forms and types, etc. It is likely that at the third stage of Metaverse development, a number of objects, such as avatars, electronic identities, virtual digital works of the ASI class, and digital humanoids, will be transferred to the category of subjects, since at the legislative level they will be endowed with certain rights and obligations inherent only to subjects.

1 Özkahveci, E., Cívek, F., & Ulusoy, G. (2022). The place of the metaverse (fictional universe) in the Industry 5.0 era. *Journal of Social, Humanities and Administrative Sciences, 8*(50), 398–409. https://doi.org/10.31589/joshas.92.

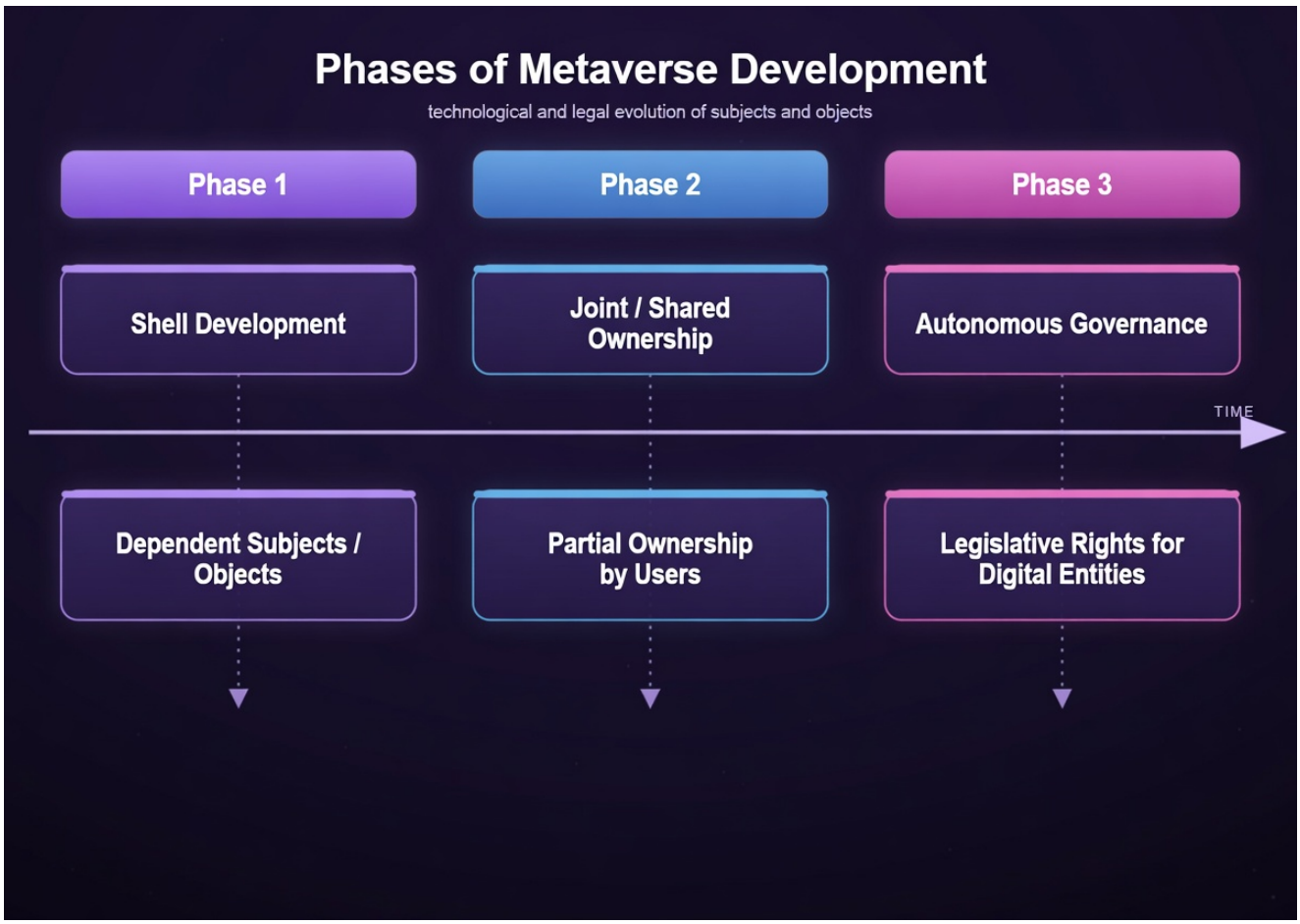


Figure 16. Metaverse: phases of development.

Currently, the Metaverse is in the initial stages of its formation and development (Özgökçeler, 2021)[1] avatars or digital identities (Kostenko, 2022b)[2], and this reduces trust in the Metaverse as a whole and leaves the ground for abuse and offence.

In our opinion, in the near future, the Metaverse will be more structured and will consist of the following elements: Personal Metaverse (Personal Metaverse, PM), Collective Metaverse (CM), Corporate Metaverse (Corporate Metaverse CorpM), Confederate Metaverse (CfM), State Metaverse (SM) and Mega Metaverse (MMV/WM) (Figure 17).

1 Özgökçeler, D. (2021). The methods and ways of implementation of the metaverse concept that can be transferred to the general audience of its cultural and commercial potential. *Academia.edu*. https://www.academia.edu/70076301

2 Kostenko, O. (2022). Electronic jurisdiction, metaverse, artificial intelligence, digital personality, digital avatar, neural networks: Theory, practice, perspective. *World Science, 73*(1), 1–13. https://doi.org/10.31435/rsglobal_ws/30012022/7751.

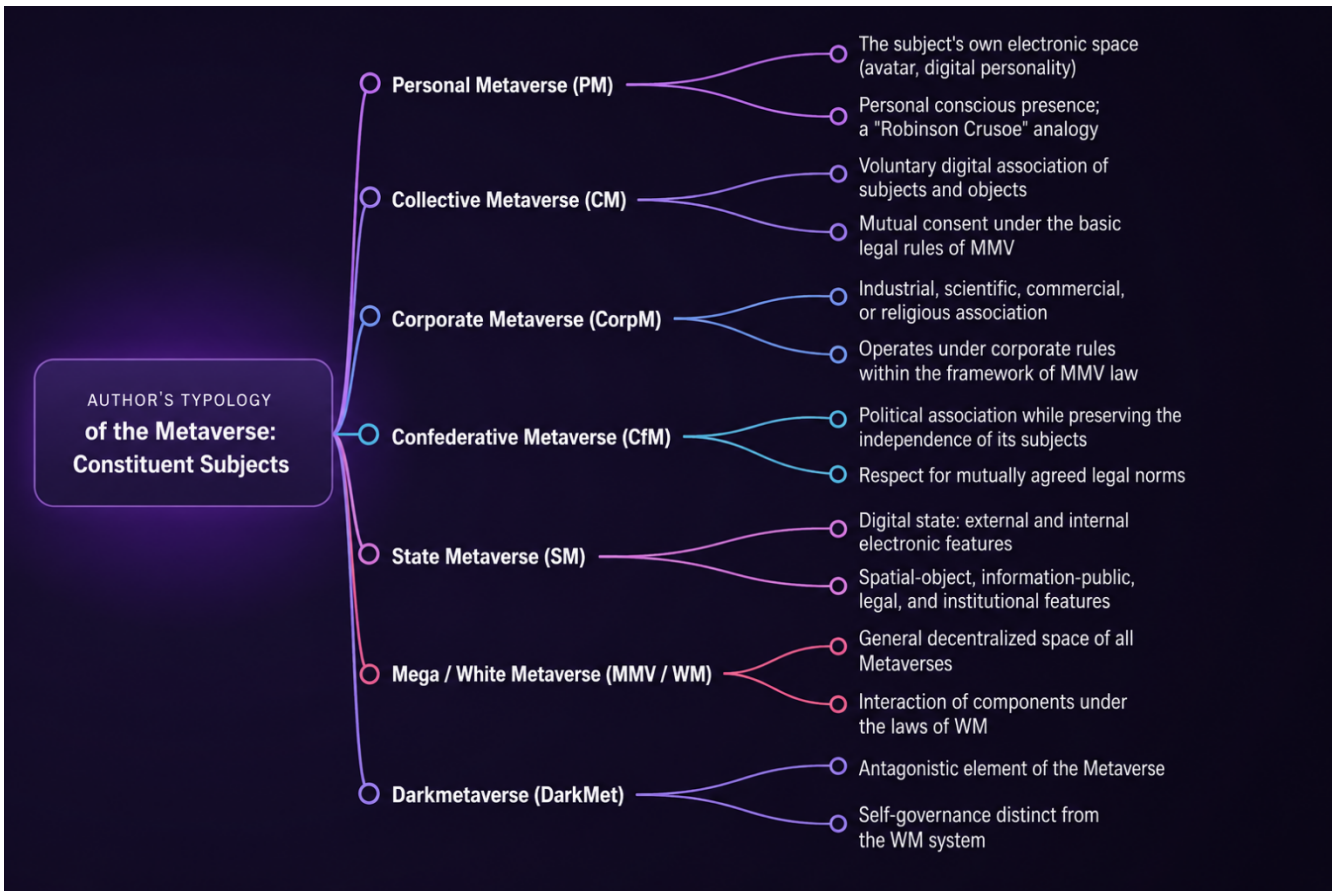


Figure 17. Metaverse: constituent entities.

Personal Metaverse (PM) means that each subject (Metaverse participant) can create their own electronic Metaverse (avatar, digital humanoid, digital personality) according to their own imagination and be in it consciously and exclusively personally, for example, by analogy with the novel "Robinson Crusoe" by the English writer Daniel Defoe.

Collective Metaverse (CM) — a voluntary digital association of Metaverse entities and objects that operates by mutual agreement, but with mandatory compliance with generally accepted basic requirements or rules of MMV law.

Corporate Metaverse (CorpM) — a voluntary, industrial, scientific, commercial, religious, or other electronic association of Metaverse entities and objects that operates under corporate rules, as long as they do not contradict generally accepted basic requirements or MMV rules.

The Confederal Metaverse (CfM) is a political association of Metaverse entities and objects, each of which retains its independence, and all together respect mutually agreed upon norms of law.

The state Metaverse (SM) is a digital state that has external and internal electronic characteristics of the state, as well as electronic subject-spatial, information-public, regulatory and institutional features.

Mega Metaverse or White Metaverse (MMV or WM) — is a common decentralised electronic space in which there are many personal, collective, corporate, confederal and state Metaverses that interact with each other according to the laws of WM (Figure 18).



Figure 18. Mega Metaverse/White Metaverse (MMV or WM).

It is expedient in the Metaverse to also provide for the possibility of the existence of the DarkMetaverse (DarkMet) as a necessary antagonistic element of the Metaverse, in which subjects, objects and the Metaverse can be concentrated with a system of self-government different from that adopted in WM.

Since the Metaverse is seen as an information and communication social ecosystem that creates, maintains, develops, and ensures the functioning of social relations in an

electronic virtual form, it is pertinent to note that the "digital jurisdiction" of the Metaverse — is a complex branch of law that regulates the social relations that constitute its subject — social relations in the Metaverse, for example, between the Metaverse and the physical world (Wyss, 2021)[1]. Each subject will have a personal unique avatar, and the subjects/objects will have unique ownership passports. Subjects and objects can carry out various types of activities — financial, scientific, creative, social, public, etc.

For example, the Republic of Barbados announced the opening of its virtual embassy in the Metaverse in 2021, and its diplomatic complex is under construction in Decentraland. Barbados' ambassador to the United Arab Emirates argued that "governments can act together when land is no longer physical land and constraints are no longer part of the equation." He also noted that small countries do not have the physical and financial capacity to support 197 diplomatic missions around the world, but the Metaverse provides parity with large countries such as America or Germany. Other countries also have experience with virtual embassies — Sweden and Estonia have opened embassies in the Second Life Metaverse.

The United Arab Emirates has already become a leader in the Metaverse, building a modern digital economy, implementing policies, and developing regulatory frameworks in areas such as virtual assets, artificial intelligence, and data protection.

Thus, the UAE's state regulatory body, the Dubai Virtual Asset Management Authority (VARA), has opened a representative office in the virtual world of The Sandbox, which will work with the private sector and relevant government agencies to create a legislative and supervisory framework for digital assets. In addition, anti-money laundering and cross-border transaction tracking regulations will be developed to ensure transparency and security for businesses and investors. Digital assets such as cryptocurrency, non-fungible digital assets, tokens (NFTs), etc., will be supported by a single legislative and regulatory framework.

Emirates Airlines has announced the creation of a brand in the field of Metaverse (Emirates Metaverse), as well as collectible and useful non-fungible tokens for its customers and employees. Also, the Metaverse has the world's first customer service centre, developed by the UAE Ministry of Health and Prevention.

As reality shows, social relations in the Metaverse are created, established, and developed despite the skepticism of individual scientists, experts, and politicians.

1.4.14. Problems of Legal Regulation of Public Relations in Web 2.0-Web 3.0

The starting methodological position is that Web 2.0-Web 3.0 is not only a set of "social Internet" technologies, but an institutionalised communication-given space in which social interactions (content, profiles, communities, advertising and analytical models) acquire legal relevance through their connection with rights, duties and responsibilities. In view of the above, the legal understanding of Web 2.0-Web 3.0 within the framework of information law should focus not on the technical description of

1 Wyss, J. (2021, December 14). Barbados is opening a diplomatic embassy in the metaverse. *Bloomberg*. https://www.bloomberg.com/news/articles/2021-12-14/barbados-tries-digital-diplomacy-with-planned-metaverse-embassy.

services, and on the construct: sources of regulation - subjects - objects - legal facts - liability - proof - transboundary (Pu et al., 2022)[1].

Sources of regulation Web 2.0-Web 3.0.

The regulatory model Web 2.0-Web 3.0 is multi-level and mixed, as it combines public and private law sources, as well as "quasi-normative" technical standards, which de facto perform the function of procedural specification of duties. In terms of information law, we are talking about a complex construction of "law - procedures - technical guarantees", in which the text of the norm is only the apex of the regulatory mechanism, while the effectiveness of the regime is determined by the possibility of its implementation through the interface, event logs, access rules and accountability of intermediaries.

The public law core of Web 2.0-Web 3.0 is formed, firstly, by constitutional guarantees and principles: the right to respect for private life, freedom of expression, freedom of association, the right to judicial protection and fair procedure, the prohibition of discrimination. It is these guarantees that set the "red lines" for any moderation, profiling, and access restriction models, even if such restrictions are implemented by a private platform. In this context, the European Convention Doctrine of Balance between Freedom of Expression and Protection of Privacy/Reputation (Standards for the Interpretation of Articles 8 and 10 of the ECHR) is significant, which actually functions as a supranational "corrector" of state policy in the digital sphere.

Secondly, at the level of sectoral legislation, Web 2.0-Web 3.0 is regulated by an array of norms covering: personal data protection and privacy; electronic communications and network services; e-commerce and consumer protection; cybersecurity and incident management; intellectual property and content liability regimes; advertising rules, child protection and prevention of violence/hatred. In EU law, this block has a high level of codification: the basis for privacy is the GDPR, which fixes the principles of legality, transparency, minimisation, and targeted use of data. In the field of cybersecurity, NIS2 is key, which sets requirements for organisational measures and reporting significant incidents.

Thirdly, for the legal architectonics of Web 2.0, the EU "platform" block: the Digital Services Act (DSA) as a framework of responsibilities and transparency/moderation procedures (in particular, due to reporting requirements, oversight and enhanced responsibilities for large services) is of fundamental importance. A historical prerequisite for this direction is the E-Commerce Directive 2000/31/EC, which established "liability exemptions" for certain functions of intermediaries (mere conduit/caching/hosting), thereby institutionalising the category of "limited intermediary liability" for third-party content for information law as a basic compromise between freedom of communication and protection of rights.

Fourthly, the economic and legal "framework" of Web 2.0-Web 3.0 is reinforced by the norms of competition and market regulation of digital ecosystems. In particular, the Digital Markets Act (DMA) forms a special regime for gatekeeper platforms and indirectly affects how access to the market for applications, advertising, analytics and

1 Pu, Q. L., Pang, Y., Peng, B., Hu, C. J., & Zhang, A. Y. (2022). *Metaverse report—Future is here: Global XR industry insight*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-metaverse-report-en-220321.pdf

data is organised in the Web 2.0-Web 3.0 environment. Equally important are the rules of electronic communications, since Web 2.0-Web 3.0 is structurally dependent on network infrastructures and connection quality; in EU law, this segment is systematised in the European Electronic Communications Code (EECC).

Fifth, the comparative dimension of the sources of regulation between Web 2.0 and Web 3.0 demonstrates a different logic in the United States, where the central element has long been Section 230 (47 U.S.C. § 230), which grants limited immunity to providers of "interactive computer services" for liability for third-party content and at the same time supports "good faith" moderation. It is not a "universal standard", but an important comparative model: it explains why the institutional balances between freedom of expression, private moderation coercion and judicial review can differ significantly in different legal orders, although the technological basis of Web 2.0-Web 3.0 is similar.

At the same time, Web 2.0-Web 3.0 cannot be correctly described without a private law layer, which in practice is often the "first line" of regulation. These are terms of service, community rules, moderation policies, advertising policies, privacy policies, API terms and licensing models for developers, as well as internal complaint and review mechanisms. In the field of information law, these documents should be qualified not as "secondary texts", but as normative and procedural tools of platform governance, through which the rights of access, communication, monetisation and reputation are implemented (or blocked). It is the private layer that "translates" abstract public law standards into operational procedures: notification, recording of violations, sanctions, appeals, restoration of access.

A separate group of sources is "soft law" and technical standards, including codes of conduct, regulatory guidelines, best practices, as well as risk and safety management standards. Their legal force varies, but in Web 2.0-Web 3.0 they act as a "procedural bridge" between law and enforcement: standards formalise the proper level of organisational measures, transparency, auditing, incident response, which can later become a criterion of due diligence/good faith or an element of compliance.

Thus, it can be stated: in Web 2.0-Web 3.0, law exists as a distributed system of norms and procedures, where the state sets the limits of interference, human rights guarantees and minimum standards of due process, while platforms (as information intermediaries) act as the primary regulator of access and the primary moderator of behaviour through rules, interfaces and technical "contours" of what is allowed. In this sense, Web 2.0-Web 3.0 is a complete model of "platform-legal co-governance", which methodologically leads to further analysis of the Metaverse: if in Web 2.0-Web 3.0 the procedures only supplement the norm, then in immersion environments the procedural and technical component claims to be the core of legal certainty.

1.4.15. Subjects of legal relations in Web 2.0-Web 3.0.

It is advisable to characterise the subject composition of Web 2.0-Web 3.0 as a multi-level system of roles, in which not only "who is the participant" is of legal importance, but also what function it performs in the chain of creation, transmission, moderation, monetisation and preservation of the digital footprint (Figure 19). Unlike the classical information relations "source - consumer", Web 2.0-Web 3.0 produces legal relations of the "network type", where one act (publication, complaint, targeting, blocking, leakage)

objectively "passes" through several subjects and forms different arrays of rights and obligations for them. That is why, within the framework of information law, Web 2.0-Web 3.0 is more correctly described through the functional-role classification of subjects, and not through a simple list of "users/platforms/state".

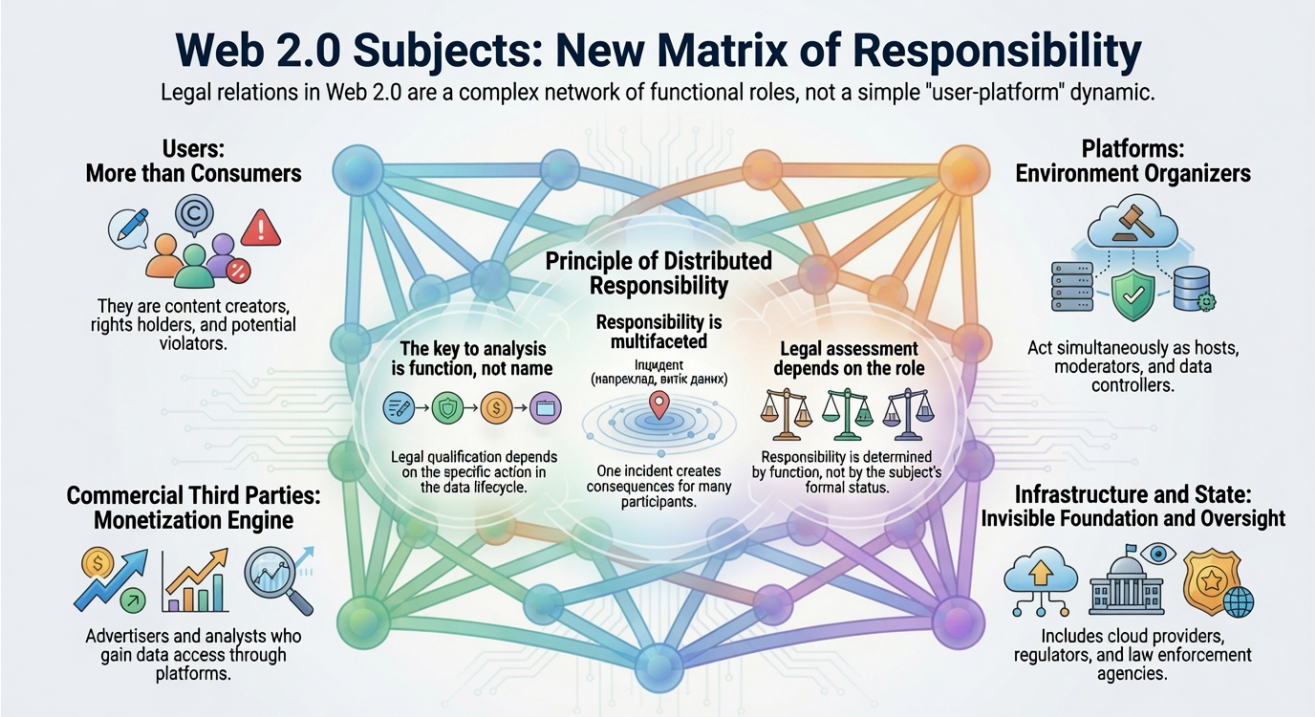


Figure 19. Metaverse 2.0: composition of entities

Firstly, primary private entities (users) cover both individuals and organisational users (business, media, institutions), as well as professional actors (content makers, community administrators, e-commerce sellers). Their legal position is multidimensional: they are at the same time a party to the accession agreement for access to the service; bearer of subjective rights in the field of data and privacy; potential author/copyright holder of the content; potential tortious infringer (defamation, copyright infringement, fraud, etc.); consumer of digital services with appropriate guarantees. It is important to note that in Web 2.0-Web 3.0, the "user identity" is often functional rather than passport: the user can act under a pseudonym, through a group, through a brand page, or through delegated access. In view of the above, information law here actually operates not only with a "person", but also with a profile/account as a legally relevant point of attribution and access to eligibility.

Secondly, platforms and service providers in Web 2.0-Web 3.0 act as organisers of the environment and at the same time bearers of obligations that are of a mixed nature: contractual (to the user), tort (for improper security or unfair practices) and public law (compliance with data requirements, security, transparency of certain procedures, interaction with competent authorities). For dissertation accuracy, it is advisable to distinguish between at least three sub-roles within this group: hosting/content intermediary (hosts and distributes UGC); a provider of an interaction platform (social network, marketplace, video hosting), which determines the rules of communities and moderation procedures; a provider of data processing tools (analytics, advertising

account, profiling), which can act as a controller, co-controller or processor depending on the configuration. It is the "stratification" of the platform into legal roles that is the key to the right responsibility: the same company can perform several roles at the same time, and then the legal assessment should be "role-based" and not general.

Thirdly, a significant place is occupied by commercial third parties that monetise or serve the Web 2.0-Web 3.0 ecosystem. These include advertisers and media buying structures, affiliate marketing networks, analytics providers, SDK providers, app and module developers, payment infrastructure operators and fintech intermediaries, and affiliate administrators. Their legal specificity lies in the fact that they often gain access to data not as direct parties to the user contract, but as counterparties of the platform or as "connected" participants in the advertising and analytical circuit. In information law categories, this is a typical situation of a "split chain of responsibility": the user interacts with the platform, but the actual data processing and influence on behaviour can occur through a network of counterparties, which requires the legal qualification of roles (controller/processor/joint controller; data recipient; subcontractor) and the establishment of a transparent reporting and accountability regime.

Fourth, it is necessary to distinguish infrastructure actors (backbone actors), without which Web 2.0-Web 3.0 does not function, but which often remain "in the shadows" in popular descriptions. These are cloud resource providers, CDNs, domain name operators, registrars, hosting providers, network infrastructure operators, and sometimes cyber security (WAF, anti-DDoS), backup, and logging providers. In a legal sense, they do not always have a direct relationship with the end user, however, their role is critical for maintaining an evidentiary trail, security, and meeting incident obligations. This is where the classical logic of information law comes into play: the legal regime of information and data depends on who has technical control over access, preservation, and integrity — even if this control is carried out "under contract" in B2B chains.

Fifth, a separate group should be "trust-service actors" — entities that provide electronic identification, authentication, certification, attribute confirmation, as well as access control tools (SSO, multi-factor authentication, account verification). They form the legal basis for attribution of actions, and therefore the basis for liability and proof. Within the framework of information law, this corresponds to the thesis that "trust" is not a psychological category, but a legal infrastructure that creates a reproducible connection between the action and the subject. That is, the evolution of Web 2.0-Web 3.0 shows that without trust providers, the platform is forced to compensate for the attribution deficit with excessive surveillance (advanced tracking) or excessive sanctions (strict moderation), which legally increases the risks of privacy and proportionality violations.

Sixth, state actors in Web 2.0-Web 3.0 are not reduced to "courts" or "law enforcement agencies": it is advisable to distinguish between regulators (data surveillance, telecommunications, advertising, competition, consumer protection), cybersecurity authorities (response coordination, security standards, incident reporting), law enforcement agencies (crime investigations, data requests), courts (control of restrictions on rights, dispute resolution, evaluation of evidence), as well as enforcement bodies (including in cross-border scenarios). In the legal ontology of information law, this means the transition from "the state as the sole arbiter" to the "state as a system of

supervision and procedures", where each authority has its own competence and its own procedural framework for accessing data, imposing duties and applying sanctions.

Seventh, the key doctrinal category for describing the subject composition of Web 2.0-Web 3.0 is distributed responsibility and the associated criteria of legal assessment: the initiator of the action, the degree of control over the environment, the predictability of risk, the possibility of prevention, due diligence, transparency of procedures and the availability of review mechanisms. The same incident (for example, illegal content or data leakage) forms a multitude of legal consequences: for the user, the limits of freedom of expression and tort liability; for the platform — response obligations and procedural safeguards; for advertising circuit — liability for unfair practices and lawfulness of processing; for infrastructure — issues of technical integrity and logs; for the state, it is a matter of the legality of requests and the proportionality of interference. That is why the dissertation analysis should "tie" subjectivity not to abstract names of participants, but to roles in the life cycle of data and content.

Summing up, it is advisable to present the subject composition of Web 2.0-Web 3.0 as a "matrix of roles", where the legal qualification depends on the function: creates/distributes content; administers the rules; processes data; provides identity and trust; provides infrastructure; carries out supervision and coercion. In our opinion, this approach is of direct methodological importance for the following sections on the Metaverse: if in Web 2.0-Web 3.0 distributed responsibility is a consequence of platforming and datacentricity, then in immersion environments it is strengthened even more due to the "density" of attribution, biometric and spatial data, the economics of virtual assets, and protocol interoperability.

1.4.16. Objects of Legal Regulation in Web 2.0-Web 3.0.

In this study, it is advisable to proceed from the fact that the "object" in Web 2.0-Web 3.0 is not abstract "information" as such, but a legally relevant digital phenomenon to which rights, obligations, prohibitions and protection procedures are directed. In other words, Web 2.0-Web 3.0 forms a multiplicity of objects that cross the boundaries of branches of law: informational, civil, administrative, criminal, consumer, as well as intellectual property law (Figure 20). In view of the above, the correct classification of objects is not descriptive, but methodological: it depends on it whether the legal regulation will be precise (targeted), or dispersed and declarative.



Figure 20. Metaverse: classification of digital objects.

Firstly, content in Web 2.0 should be understood as a complex object that simultaneously has an intellectual and legal dimension (copyright, related rights, licensing, derivative works, the right to a name/inviolability of the work) and a tort law dimension (dissemination of false information, infringement of honour and dignity, violation of privacy, hate speech, calls for violence, fraudulent messages). For information law, it is important that the content in Web 2.0-Web 3.0 is "alive" — it is continuously modified (comments, remixes, reposts, quotations, reactions), and therefore the legal assessment often depends not on a single message, but on the context of distribution and the "chain of re-posting". This is where the need arises to distinguish between primary publication, secondary reproduction and algorithmic "amplification" of coverage as different legally significant regimes.

Secondly, personal data and metadata in Web 2.0-Web 3.0 constitute a separate class of objects that is not reduced to "last name and phone number". This includes profile data, behavioural patterns, location, network identifiers, device parameters, timestamps, interaction histories, and derived indicators (audience segments, interests, probable age, etc.). The legal specificity of this object is that it has a dual nature: at the same time it is a subject of privacy and information security and a resource of economic value (targeted advertising, analytics, optimisation of services). In terms of information law, this means that regulation should cover not only "data", but also operations on data: collection, correlation, profiling, transfer, storage, deletion and recovery, since it is the transactions that produce risks of discrimination, invasion of privacy or unfair influence on behaviour.

Thirdly, it is advisable to qualify an account/profile in Web 2.0-Web 3.0 as a legally significant "access node" that combines attribution of actions, access to functionality, and accumulation of digital capital (content, subscribers, transaction history, rating). It is important that an account is not a "thing" in the classical sense, but it forms a legitimate interest of a person who needs legal protection: the right to restore access, protection from

unlawful interference, predictability of blocking procedures, proper notification and the ability to appeal against restrictions. That is why restricting or blocking an account in Web 2.0-Web 3.0 is a legally sensitive action: it affects not only the "usability", but the implementation of a number of rights, including professional activities, market access, exercise of creative rights and maintaining reputation.

Fourthly, digital reputation (ratings, reviews, statuses, "verification tags", history of violations) appears as an intangible object with clear property and social consequences. Its legal feature is a combination of two planes: protection of honour, dignity and business reputation as classic non-property benefits and economic conversion of reputation into income, access to orders, the level of customer trust, the cost of advertising, and the possibility of monetisation. For information law, the issue of procedural fairness is fundamental here: if the rating is formed algorithmically or through moderation decisions, then the reputation becomes dependent on the rules of the platform, the transparency of the criteria and the possibility of review.

It is believed that digital reputation should be interpreted as the "legal equivalent of social capital" in an information-given environment, since it functions as a tool for access to opportunities and resources, and not only as an assessment of "sympathies".

Fifth, digital assets and digital consumer objects (virtual goods, subscriptions, internal currency units of services, paid functions, digital gifts) form a segment where the object of regulation is not "information", but property and economic goods presented in digital form. Here, the constructions of contract law and consumer protection become key: proper quality of the digital service, transparency of conditions, right of withdrawal/return (where applicable), prohibition of unfair practices, distribution of the risk of technical failure or compromise of access. It is important that such assets often have limited sovereignty: they exist within the framework of the platform's rules and can be modified by it, and therefore the object of regulation is also the "constancy" of the user's eligibility, the predictability of changes and the limits of unilateral intervention of the provider.

Sixth, the standalone (and often underestimated) object of Web 2.0-Web 3.0 is the algorithmic profile and results of automated ranking/recommendations. The legal relevance here lies in the fact that the algorithm shapes the visibility of content, the accessibility of the audience, the risks of informational damage, and the intensity of commercial impact. In information and legal optics, this means that the object of regulation becomes not only "content", but also the mode of its distribution: to whom, when, with what intensity, on the basis of what criteria, and whether these criteria do not contain discriminatory effects. That is why, at the level of doctrine, it is advisable to distinguish between "content as message" and "content as controlled visibility" — the second aspect is especially important for assessing manipulation, political advertising, covert influence and unfair competition.

Seventh, in Web 2.0-Web 3.0, a separate class of objects is a digital trace/event logs (logs, access metadata, technical records of interactions), but here it is important to keep the focus on "objectivity", and not on proof as a procedure. Event logs are subject to regulation because they determine: the limits of permissible collection and storage; integrity and security requirements; access of competent authorities; the ability to reproduce the event in controversial situations. In the field of information law, this is a

continuation of the classic problems of the regime of information resources: who has the right to access journals, on what grounds, in what period, and how to prevent the transformation of journaling into an instrument of excessive surveillance.

Eighth, the evolution of Web 2.0-Web 3.0 from an "information resource" to an "information-given environment" means that the object of regulation is increasingly becoming a mode (access, visibility, moderation, storage, transmission), rather than a single artifact. This leads to an important doctrinal consequence: information law must operate not only with the categories of "message/data", but also with the categories of context and architecture — that is, the conditions that make information interaction legally significant or legally dangerous. It is the "mode" of objects in Web 2.0-Web 3.0 that is the bridge that allows you to move correctly to the Metaverse in the future: there, objects are increasingly becoming not just data and content, but "presence", "behavioural environment" and "contextual privacy", which require an even more subtle legal ontology.

1.4.17. Legal procedures Web 2.0-Web 3.0.

For Web 2.0-Web 3.0, the key is that it transforms the classical notion of a legal fact as a "life circumstance" that occurs outside the law: in the digital environment, a legal fact is increasingly an action-procedural construct, i.e. a combination of action/state, technical fixation, rule (normative or platform) that gives this action legal significance, and evidentiary reproducibility. Therefore, in Web 2.0-Web 3.0, it is correct to speak of "legal facts-interface events" and "legal facts-log entries", which acquire legal consequences precisely because the environment is able to identify, record and compare them with the legal regime (Figure 21).

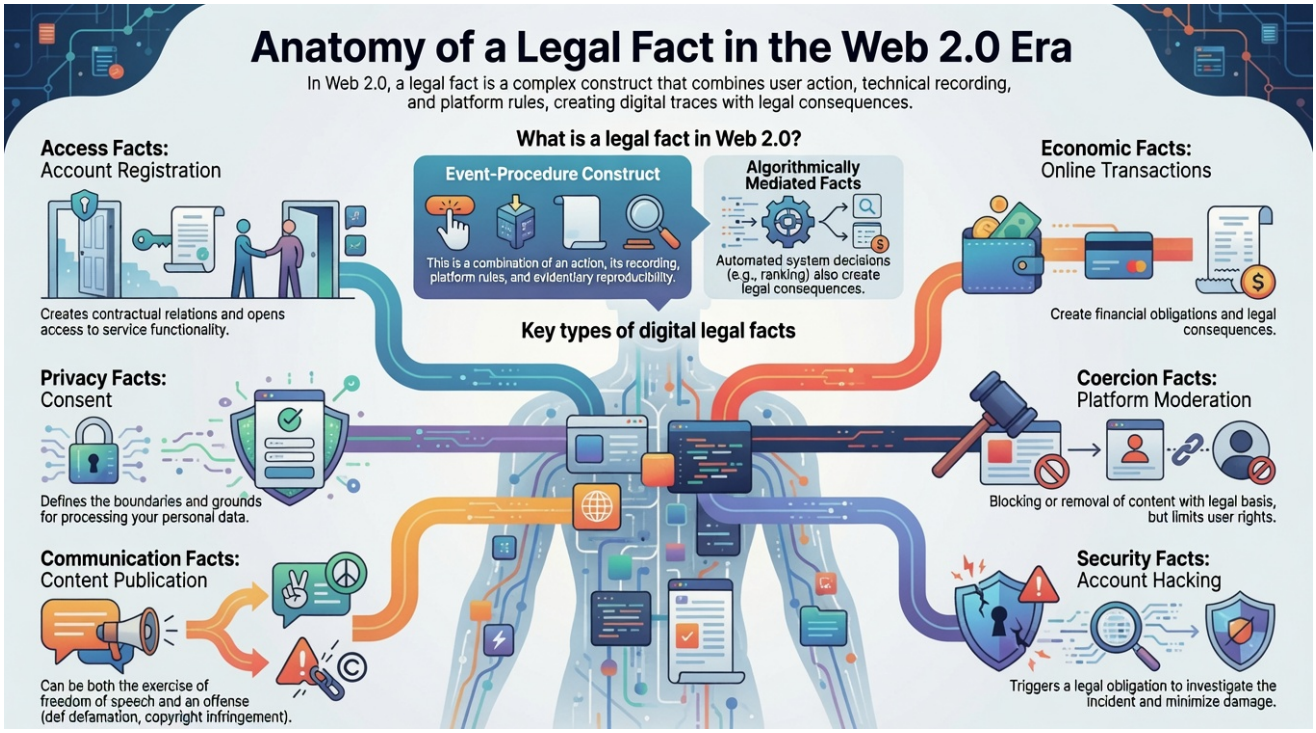


Figure 21. Metaverse: Legal Fact as an Actionable Procedural Construct.

Firstly, the basic legal fact in Web 2.0-Web 3.0 is the entry into a digital legal relationship of access through account registration or joining the service. It is not only about "creating a profile", but about the emergence of a set of mutual rights and obligations: the user acquires the authority to use the functionality, and the provider acquires legal grounds for providing the service, applying the platform's rules and (within the legal framework) processing certain categories of data. In this act, the "threshold" nature is important: it opens the mode of applicability of contractual terms, privacy policies, moderation rules and sanctions mechanisms. In information and legal optics, this is the "entry point" into the regulatory circuit Web 2.0-Web 3.0, where legal certainty depends on the transparency of conditions, awareness and the ability to control settings.

Secondly, a legal fact of a special type is the provision of consent or the establishment of privacy settings that form (or change) the grounds and limits of data processing. Here, Web 2.0-Web 3.0 demonstrates a characteristic feature: the expression of will is often carried out in the format of "click-wrap" or "control of the settings panel", and the legal consequences can be significant and long-lasting. Not only the act of "agreed" is legally important, but also its parameters: scope, purpose, term, possibility of revocation, consequences of refusal. That is why it is advisable to describe consent as a procedural legal fact consisting of informing, choosing and fixing, and not as a one-time declaration.

Thirdly, the central group of legal facts in Web 2.0-Web 3.0 are the acts of creating, distributing and modifying content: publishing, commenting, reposting, citing, remixing, streaming, reacting. Their legal specificity lies in duality: it is both the exercise of freedom of expression (information activity) and the potential occurrence of corpus delicti or grounds for civil protection (copyright infringement, invasion of privacy, defamation, incitement to violence, etc.). It is important to note that in Web 2.0-Web 3.0, legal significance often depends on the "mode of distribution": initial publication, redistribution, and algorithmic amplification of coverage have different factual consequences, and therefore require a differentiated legal assessment. In our opinion, this is where the "ecology of the legal fact" manifests itself: in Web 2.0-Web 3.0, the fact gains intensity due to the network effect, and the legal risk does not grow linearly, but exponentially along with the coverage.

Fourthly, the key legal facts include electronic transactions and transactions within services: subscription, payment, purchase of a digital product or service, connection of paid functionality, donations, advertising. They certify that Web 2.0-Web 3.0 is not only a communication, but also an economic environment where obligations, consumer guarantees, return rules (where applicable), liability for improper service provision and protection against unfair practices arise. The peculiarity of Web 2.0-Web 3.0 is that a transaction is almost always accompanied by a set of technical facts: identification of the payer, timestamps, records of the payment provider, access logs; It is they who ensure the reconstruction of the legal fact in the dispute.

Fifth, specific for Web 2.0-Web 3.0 is a group of legal facts of platform governance, i.e. moderation and compliance actions: content removal, visibility restrictions, account blocking, demonetisation, "warnings", content labelling, age verification, application of anti-fraud restrictions. These actions are legally significant because they change the scope of the user's powers (access, communication, economic activity) and form the provider's

obligation to act in good faith, proportionately and procedurally correct. In the dissertation, it is advisable to emphasise that the moderation act is not a "technical setting", but a legal event that must have minimally sufficient procedural attributes: notification, motivation, possibility of appeal, review and fixation of grounds.

Sixth, a separate category is formed by security incidents and violation of the integrity of the digital environment: account compromise, unauthorised access, data leakage, content substitution, social engineering, hacking of advertising accounts, attacks on supply chains. Legally, such events give rise to a range of consequences: from tort liability for the damage caused to the obligations to report the incident, investigate, restore access, minimise damage and implement corrective measures. In the plane of information law, an incident is a legal fact because it "switches" the mode: from normal functioning to response mode, where event logs, forensics and evidence of the actions of the parties become important.

Seventh, fundamentally important for Web 2.0-Web 3.0 is the thesis about the emergence of legal facts at the intersection of law and architecture. Pressing a button, selecting settings, automatic ranking, recommendation, triggering an anti-fraud trigger — all this can generate legal consequences. Here it is appropriate to formalise the concept of an algorithmically mediated legal fact as such: arises due to an automated decision or an automated action of the system; affects the rights/obligations of a person (access, visibility, monetisation, reputation, security); needs to be reconstructed through event logs, rule parameters, and the context of decision-making. Algorithmically mediated facts are the "stress points" of information law, since they combine technological opacity with the legal requirement of motivation and predictability.

Eighthly, from a methodological point of view, in Web 2.0-Web 3.0, it is advisable to group legal facts not only by content (registration, consent, publication, etc.), but also by legal function:

1) access facts (login/identification/recovery),
2) privacy facts (consent/withdrawal/restriction of processing),
3) facts of communication (propagation/visibility/labelling),
4) facts of the economy (transactions/payments/subscriptions),
5) facts of coercion (moderation/sanctions/appeals),
6) security facts (incidents/investigations/recovery).

Such grouping, based on the analysis, allows us to show that Web 2.0-Web 3.0 is an environment in which law "works" through events that necessarily have a digital footprint, and therefore require standards of logging, preservation and accountability.

Summing up, the legal facts of Web 2.0-Web 3.0 constitute an event-procedural complex in which the legal consequence arises not only from the "action" of the user, but also from the architectural and algorithmic procedures of the platform. This feature is a methodological bridge to the Metaverse: there, legal facts become even more "environmental" in nature (identity, logging, spatial events, biometric parameters), and therefore the doctrine of Web 2.0-Web 3.0 can be used as a preliminary level of legal ontology for digital jurisdiction.

1.4.18. Responsibility in Web 2.0.

Liability in Web 2.0 should be understood as a hybrid system of legal consequences arising from the violation of legal norms or rules of the platform, and combining tort, contractual and public law components. It is fundamentally important that Web 2.0-Web 3.0 changes the classic scheme of "violator → victim → court": in a platform environment, there is often an intermediate circuit between infringement and restoration of the right — platform governance (moderation, anti-fraud, access restriction), which can ensure a quick end to harm, but at the same time creates risks of private coercion without due process. In view of the above, liability in Web 2.0-Web 3.0 is not only a sanction, but also a risk management mechanism that requires procedural guarantees and a clear delineation of roles.

Firstly, the responsibility of the user in Web 2.0-Web 3.0 covers a set of possible legal regimes, depending on the nature of the act and the consequences. At the private law level, this is, first of all, civil (tort) liability for:

a) encroachment on non-property rights (honour, dignity, business reputation, privacy, images, personal data);

b) violation of intellectual property rights (illegal reproduction/distribution, plagiarism, circumvention of technical means of protection);

c) unfair practices in digital interactions (misleading ads, phishing messages, manipulative schemes);

d) causing property damage due to fraudulent or unlawful actions.

In the presence of appropriate signs and public danger, the user's behaviour can go into the plane of administrative or criminal liability, which is especially typical for crimes where the digital environment is a way of committing or an environment for the implementation of intent (fraud, unauthorised access, stalking, distribution of prohibited content, etc.). An important feature of Web 2.0-Web 3.0 is that the "identity deficit" (anonymity/pseudonymity) does not deny responsibility, but complicates its implementation and shifts the centre of gravity to attribution and proof tools.

Secondly, the responsibility of the platform/provider is not reduced to the question of "is the intermediary responsible for someone else's content". In Web 2.0-Web 3.0, it has a minimum of three legal circuits. The first is contractual, which includes the obligation to properly provide a digital service: the availability of the service, the correctness of the functionality, the predictability of the conditions, compliance with the stated policies, a reasonable level of protection of accounts and the communication channel. Here, typical requirements relate to the restoration of access after compromise, protection against unlawful blocking, transparency of rule changes, as well as good faith in the application of sanctions and monetisation mechanisms.

The second circuit is public law, which covers obligations regarding the legality of data processing, ensuring information security, responding to incidents, fulfilling legitimate requests from competent authorities, as well as compliance with special requirements for the transparency of moderation or protection procedures for minors (in those legal orders where such requirements are detailed). The third circuit is tort and compliance, which manifests itself through liability for non-compliance with minimum standards of due diligence: if the platform systematically fails to implement basic security safeguards, allows obvious risks of data leakage, or creates conditions for massive rights

violations, it can be subject to legal consequences regardless of the fact that the original author of the content was the user. In other words, the responsibility of the intermediary in Web 2.0-Web 3.0 is increasingly described not by the category of "guilt for content", but by the category of negligence in risk management.

Thirdly, in Web 2.0-Web 3.0, the key problem is the distribution of responsibility among several participants in the chain (platform - advertising provider - analytics provider - module developer - cloud provider). For information law, this means the need for a doctrinal "responsibility map" according to the following criteria:

a) the degree of control over the data/content;

b) the possibility of preventing harm;

c) risk predictability;

d) transparency and documentation of processes;

e) availability of internal control mechanisms (audit, response, compliance).

In view of the above, the same event (for example, data leakage) in the legal analysis can be "decomposed" into a series of related violations: improper organisation of access, weak authentication mechanisms, insufficient encryption, lack of segmentation of accesses, untimely notification, lack of corrective measures. This approach makes liability not a "personalised legend" but a verifiable legal construct.

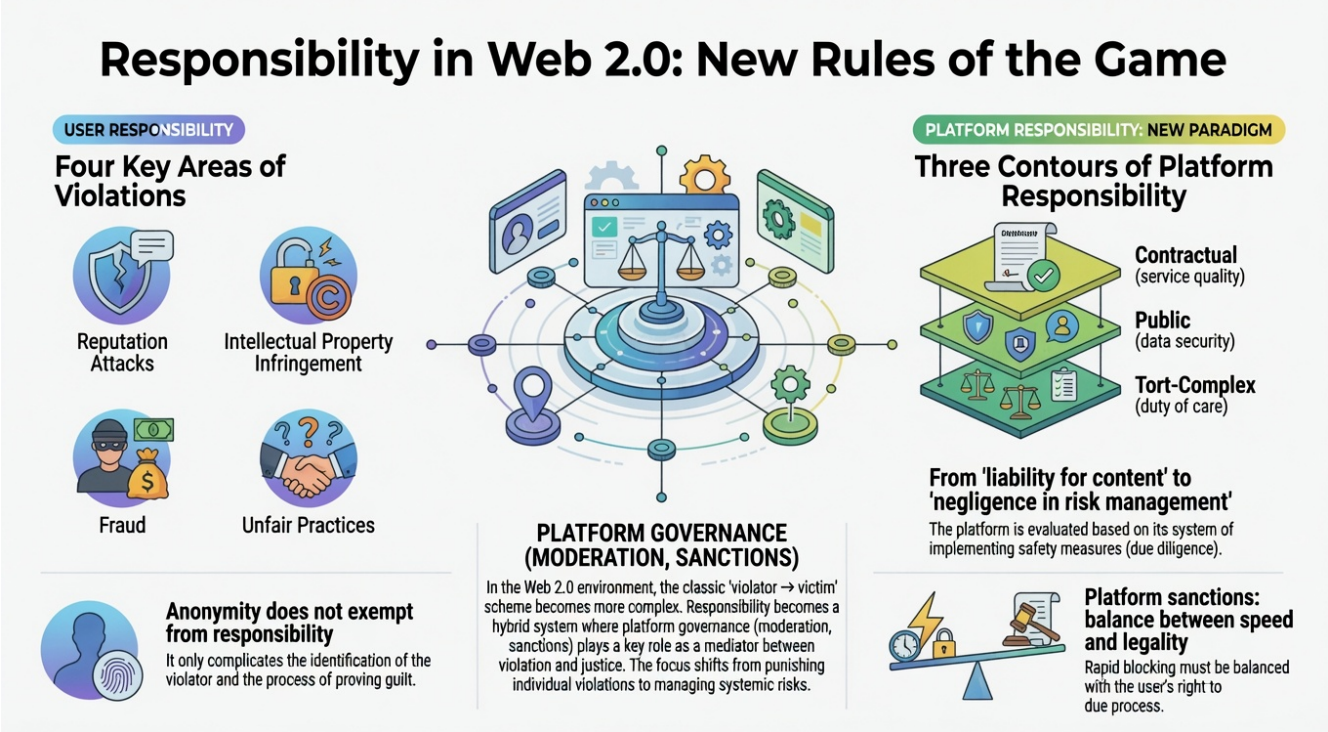


Figure 22. Metaverse: Responsibility in Web 2.0.

Fourth, a special phenomenon of Web 2.0-Web 3.0 is platform sanction as a form of private coercion. It is characterised by its duplicity: on the one hand, it performs the function of quick termination of harm (removal of illegal content, blocking a fraudulent account, limiting spam), and on the other hand, without proper procedures, it can turn into a disproportionate interference with a person's rights (access, communication, labour, entrepreneurship, reputation). That is why modern legal thought seeks to "translate" platform sanctions into the categories of due process: notification to the user, provision

of clear grounds, the possibility of objection, reasonable review terms, proportionality of the measure and restoration of rights in case of error. Platform sanction is a "point of conflict between legality and efficiency": efficiency requires speed, but legality requires procedural safeguards.

Fifth, in Web 2.0-Web 3.0, the instrumental category of due diligence is important as a criterion for assessing the behaviour of the intermediary and other participants. In practical terms, this means: whether reasonable protection measures have been implemented; whether an audit is carried out; whether there are incident response policies; whether the complaint mechanisms are working; whether systemic risks are reduced (for example, massive violations of intellectual property rights or toxic practices in communications). Legally, this makes it possible to distinguish "randomness" from "systemic negligence", as well as to transfer the assessment from the plane of moral judgments to the plane of evidentiary criteria.

Sixth, within the framework of information law, it is important to emphasise that liability in Web 2.0-Web 3.0 has not only a punitive, but also a restorative dimension: removal of illegal content, rebuttal, termination of violation, restoration of access, compensation for damages, blocking leakage, notification of victims, corrective security measures. It is the recovery mechanisms in the platform environment that are often paramount, since the speed of information dissemination makes post-factum compensation less effective compared to the prompt termination of the violation and minimisation of damage.

Seventh, based on the analysis, a general conclusion can be formulated: the model of responsibility in Web 2.0-Web 3.0 is multichannel, and its effectiveness depends on the ability to reconcile private mechanisms for stopping harm (moderation, anti-fraud, sanctions) with public law guarantees of human rights and procedural control. This node ("private coercion ↔ public guarantees") creates a methodological bridge to further analysis of the Metaverse: there, the intensity of data, the economic "cost" of interactions, and the deeper dependence of rights on the architecture of the environment will make the issue of sanction procedure and the distribution of responsibility even more acute.

1.4.20. Proof in Web 2.0-Web 3.0.

The procedural dimension of Web 2.0-Web 3.0 is one of the most "operational", since it is this stage that shows whether the law is capable of turning a digital event into a legally proven fact. Methodologically, it is important to emphasise: Web 2.0-Web 3.0 produces an excess of digital footprint, but judicial or quasi-judicial proceedings do not require an "array of data", but procedurally suitable evidentiary material, i.e. one that meets the criteria of propriety, admissibility, reliability and sufficiency. In terms of information law, this means: evidentiary value is determined not only by the content, but also by the procedure for obtaining and the possibility of verification.

Firstly, the proof in Web 2.0-Web 3.0 is based on a heterogeneous set of sources, which can be conditionally divided into:

a) content artifacts (screenshots, screen recordings, copies of messages, web archive pages, audio/video);

b) metadata and logging (timestamps, account IDs, edit histories, IP/UA data, access logs, server logs, records of anti-fraud systems);

c) transactional records (payments, subscriptions, donations, advertising accounts, logs of access changes and roles);

d) verification and attestation data (confirmation of number/e-mail, two-factor authentication, identity verification, "verification tags");

e) responses of providers (certificates, responses to requests, data issuance logs, confirmation of the fact of blocking/deletion); (f) expert opinions (computer-technical, telecommunication, linguistic, phonoscopic, etc.) on authenticity and integrity. Such heterogeneity does not require intuition from law enforcement, but a clear assessment algorithm — from identifying the source to checking the integrity and reconstruction of the event.

Second, in Web 2.0-Web 3.0, the basic thesis is that a proof is not a "file" but a reconstruction of an event. The screenshot itself is only an image of the state of the screen, while the answer to the question is legally significant: where, when, by whom and under what conditions this state was recorded; whether it corresponds to the original resource; whether there was a possibility of modification; Whether the context is saved (URLs, timestamps, profile IDs, interaction history). That is, Web 2.0-Web 3.0 gave rise to the phenomenon of "contextual proof": persuasiveness requires not only "words on the screen", but a set of circumstances that make an event reproducible and verifiable.

Thirdly, the principle of procedural suitability of the digital trace is key: the evidence must be identified, integral, reproducible and obtained in the proper way. Identification means the ability to establish the source (account, domain, service, technical node) and subject (attribution, at least at the profile/access level). Integrity requires proof of the absence of changes after fixation. Reproducibility means the possibility of re-verification by a third-party entity (court, expert) according to the same or equivalent protocol. The proper way to obtain it is to comply with the requirements of the procedural law and the limits of permissible interference with the privacy and secrecy of communications. In view of the above, "availability of data" does not equal "evidence of data": without a procedural outline, data remains a technical artifact.

Fourthly, the chain of custody is of particular importance as a legal mechanism that turns a digital artifact into evidence. In Web 2.0-Web 3.0, the chain of custody must be adapted to the nature of digital objects:

a) fixation of the primary carrier/source;

b) documenting the method of extraction or copying (export, download, API, request to the provider);

c) formation of checksums/other means of checking immutability;

d) logging of the transfer and access to the material;

e) storage in conditions that prevent modification;

f) the possibility of independent verification.

In content disputes (where material can be deleted, edited, or "drowned" algorithmically), the chain of custody is not a technical formality, but a condition for proving that this particular content existed at a specific time and had specific properties.

Fifth, proving in Web 2.0-Web 3.0 has another difficulty — the instability of digital objects. Content can be changed, edited, deleted; links can lead to another resource; access may be restricted geographically or by age; The platform can change the interface and display order. Therefore, the principle of "operational fixation" becomes important

for information law: at the time of detection of a violation, it is necessary not only to preserve the artifact, but also to record the context of existence (access conditions, account status, visibility parameters, the presence of markings, moderation reactions). In our opinion, in Web 2.0-Web 3.0, evidence actually moves from "collecting documents" to "collecting system states", which significantly increases the role of technical literacy of law enforcement and forensic tools.

Sixth, in Web 2.0-Web 3.0, there is an increasingly evidentiary inquiry not only about "what is said/done" but also about why the environment has made a certain decision. This applies to blocks, demonetisation, labelling, coverage restrictions, suspected fraud, advertising restrictions. This is where the conceptual limit of traditional proofing is revealed: classical standards work well to establish the fact of publication or access, but weaker — to test automated decisions based on profiling, model signals, and behavioural scorings. This is the "open question" of Web 2.0-Web 3.0: data became evidence, but data also became the basis for an automated management decision, and therefore proof should be extended to minimum standards of explainability (which parameters/rules were essential), reproducibility (whether it is possible to check the correctness of operation) and procedural review (an effective appeal mechanism).

Seventh. In Web 2.0-Web 3.0, part of the evidence is "in the hands" of the provider, which means that there is a need for procedural mechanisms of demand (within the framework of civil/administrative/criminal proceedings) or standardised channels of interaction with the platform. This creates tension between the two values of information law: privacy (restriction of access to data) and the right to an effective remedy (the ability to prove the circumstances). In view of the above, in the Web 2.0 model, proof is not only a technical, but also a constitutional problem of the balance of rights.

In conclusion, Web 2.0-Web 3.0 has formed a mature practice of "data as evidence" through the diversity of digital traces and the technical possibility of logging, but at the same time it has put forward a new standard: proof must confirm not only the event, but sometimes also the procedure for making a platform decision. Such a shift (from "proof of event" to "proof of algorithmic basis") is the most significant procedural example of Web 2.0-Web 3.0 and a direct prerequisite for future models of digital jurisdiction in the Metaverse, where the architecture of the environment is even more closely fused with the legal implications.

1.4.21. Cross-border and conflict issues Web 2.0-Web 3.0.

Web 2.0-Web 3.0 is extraterritorial in nature: digital data is hosted in distributed infrastructures, interaction participants are located in different states, the platform can be incorporated in one jurisdiction, and actual markets, advertising circuits, and target audiences in others. In view of this, the classic territorial reference ("place of action") loses its ambiguity, but there is a need for a multifactorial test that takes into account the place of damage, the location of the subject, the place of "targeting" of the service, the place of data processing and the place of service provision.

First, cross-border gives rise to the problem of multiple jurisdictions: the same digital event (publication, leak, fraud, blocking) can simultaneously "claim" to be considered in several legal orders. In the civil law plane, this manifests itself as a competition of forums for claims for the protection of reputation, privacy, intellectual property or damages. In the administrative and legal plane — as a competition of

supervisory powers (for example, in the field of data or cybersecurity), where one regulator can demand actions that contradict the prescriptions of another. In the criminal law plane — as a problem of territorial and personal jurisdiction over crimes committed through the network. Within the framework of information law, this forms a special phenomenon of "jurisdictional layering", when legal relations do not have a single "centre of gravity" and require coordination procedures.

Secondly, cross-border actualisation of conflict-of-laws issues of applicable law. For contractual relations (user ↔ platform), the key is the choice of law regime in the contract and the limits of autonomy of will, especially when the user is a weak party (consumer) or when it comes to the protection of personal data, which traditionally limits the freedom to choose law by mandatory norms. For torts (privacy violations, defamation, IP violations), the traditional conflict of laws link to the "place of harm" becomes variable: the damage can be diffuse (reputational damage in several countries), and its "localisation" often coincides with the place of residence of the victim or the place where the content has acquired significant coverage. With this in mind, in Web 2.0-Web 3.0, conflict of laws are forced to work with the concept of "multiple damages" and criteria for directing the service's activities to a specific market.

Thirdly, the extraterritorial effect of data norms requires a separate analysis. The object of conflicts here is not so much the "right to content" as the control over data flows: who has the right to request access, rectification, deletion, restriction of processing; which authorities can impose fines; whether data transfer to a third country is allowed; how legal compliance is ensured in B2B processing chains. That is, Web 2.0-Web 3.0 has formed the "geopolitics of data" as a legal phenomenon: data is at the same time an economic resource, a subject of human rights and an object of state interest (security, investigation, crime prevention). That is why conflict issues here are not only of a private law, but also of a public law nature (Figure 23).

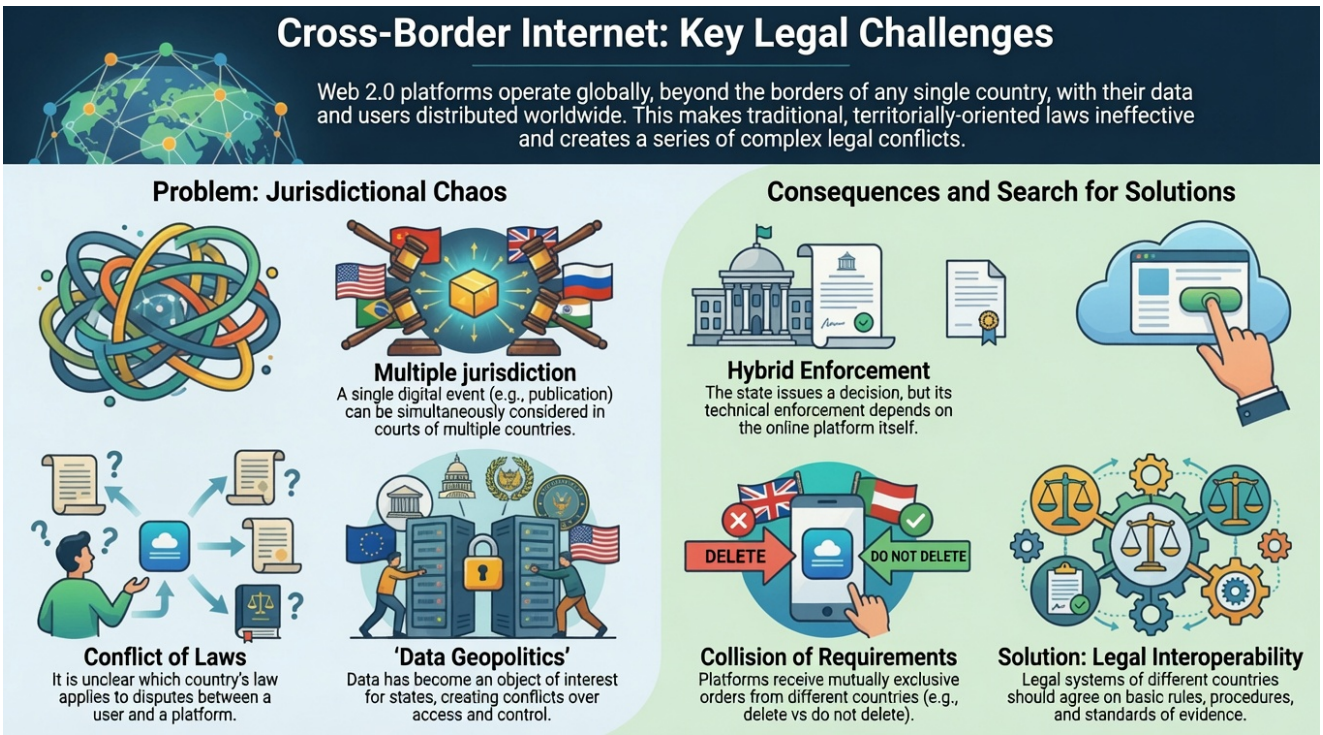


Figure 23. Metaverse and Cross-Border.

Fourthly, cross-border nature directly affects the enforcement of decisions and coercion. Even if a court or regulator makes a decision, its practical implementation in Web 2.0 often depends on whether the state has an effective channel of influence on the platform or its assets, whether there is a mechanism for international recognition and enforcement, or whether the implementation is actually "delegated" to the provider through its access and moderation tools (content removal, account blocking, monetisation restrictions). Hence a scientifically and legally important thesis: Web 2.0 gives rise to a hybrid model of coercion, where the state formulates a prescription, but technical implementation is often provided by a private entity that controls the access infrastructure and data. This hybridity is the source of "structural asymmetry": the law claims to be universal, but the enforcement tools are concentrated in the provider, which requires separate guarantees of accountability.

Fifth, cross-border disputes in Web 2.0-Web 3.0 are complicated by access to evidence. Evidence may be located in data centres of another country, be under the control of the provider, be protected by privacy regimes or secrecy of communications, and its provision may depend on mutual legal assistance procedures, on the company's internal policies, or on the use of special request mechanisms. In this context, information law faces a double requirement: to ensure effective protection of rights (to prevent "immunity through infrastructure") and at the same time not to legitimise excessive or disproportionate interference with privacy. In view of the above, cross-border evidence becomes a critical point where conflict of laws, procedural law and data regimes need to be reconciled.

Sixth, doctrinally, the cross-border nature of Web 2.0 reinforces the requirement of legal interoperability — not as an abstract slogan, but as a practical necessity. Legal interoperability in this context should be understood as the ability of different legal orders, at least at a minimum level, to coordinate:

a) standards for the admissibility and integrity of digital evidence;

b) basic guarantees of privacy and due process when accessing data;

c) requirements for procedures for responding to illegal content and security incidents;

d) criteria for the responsibility of intermediaries; (e) mechanisms for mutual recognition of certain procedural actions (e.g. authentic fixation of content or confirmation of facts by the provider).

Without such "common legality protocols", cross-border cases remain in a state of fragmentation, where each legal order sees only "its own segment" of the digital event.

Seventh, in practical terms, cross-border also means regulatory competition and risks of conflict of precepts: the platform can simultaneously receive mutually exclusive requirements (delete/not delete; provide/not provide data; localise/not localise). This gives rise to the phenomenon of "collision of compliance", when the fulfilment of the requirements of one state creates a legal risk in another. For information law, this is proof that in Web 2.0-Web 3.0 only substantive norms are not enough; Procedural coordination mechanisms and standardised channels of cooperation are needed, which reduce the space for arbitrariness and corporate "arbitrage" between legal orders.

That is, the cross-border nature of Web 2.0-Web 3.0 brings conflict issues from the periphery to the level of the methodological core: jurisdiction, applicable law,

enforcement of decisions and access to evidence in the digital sphere are interrelated and depend on control over access infrastructure and data. It is from the experience of Web 2.0 that the need to design a digital jurisdiction for the Metaverse as a cross-border interoperable system arises, where legal interoperability is enshrined not only in declarations, but in minimum standards of procedures, evidence, and accountability.

1.4.22. Problems of legal regulation of the Metaverse.

The problem of legal regulation of digital environments such as the Metaverse is that the Metaverse as an immersive medium (XR-space) gives rise to a qualitatively new configuration of social relations, where legally significant actions are carried out through digital representations (avatars), recorded by digital traces, and increasingly mediated by algorithmic and protocol mechanisms. At the same time, mass communication narratives perform the function of social legitimation and "objectification" of ideas about the Metaverse, however, in the dissertation legal analysis, they should be reduced to an auxiliary methodological layer: they show *how* society explains a new phenomenon, but do not answer the question *of what* legal regimes it determines and *what* legal consequences occur.

Therefore, it is advisable to use discourse analysis as a tool for fixing legitimisation schemes (knowledge "becomes clear", "natural", "everyday"), but the actual concept of Metaverse law should be formed through the legal ontology of relations: subjects, objects, facts, procedures and responsibilities (Popiołek et al., 2023; Dwivedi et al., 2022)[1, 2].

An important starting point is definitional pluralism. International standardisation initiatives state the presence of a large number of competing definitions: in particular, the technical documents of the ITU Focus Group on Metaverse indicate that the preparation of the standardised definition was based on the analysis of about 150 existing Metaverse definitions. For legal science, this fact has not a descriptive, but a methodological meaning: law cannot be "replaced" by one marketing or technocratic interpretation; instead, it is necessary to single out such features of the Metaverse that are legally relevant, that is, they change the regime of legal personality, object composition, evidence, and jurisdiction.

In this regard, it is advisable to distinguish the Metaverse as a technological and social configuration from individual products (game worlds, VR applications, social networks) and offer a working legal definition suitable for further normative argumentation. Generalisations emphasising: immersiveness (3D/XR experience), real-time access and persistence of the environment, interoperability or at least a tendency towards it can serve as a reference point (Figure 24).

Therefore, the Metaverse is proposed to be understood as a network (or ecosystem) of digital environments that provides persistent immersive user interaction in near real-time, with

1 Popiołek, M., Cyrek, B., Giermak, M., & Barańska, M. (2023). Technological, social and legal aspects of the metaverse in the light of the literature review. *Zarządzanie Mediami, 10*(4), 281–297. https://doi.org/10.4467/23540214ZM.22.019.17963

2 Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., ... Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542.

the potential for cross-platform interoperability and portability of digital roles/assets/data principles of digital philosophy (Kostenko et al., 2022c; Kostenko et al., 2025)[1,2].

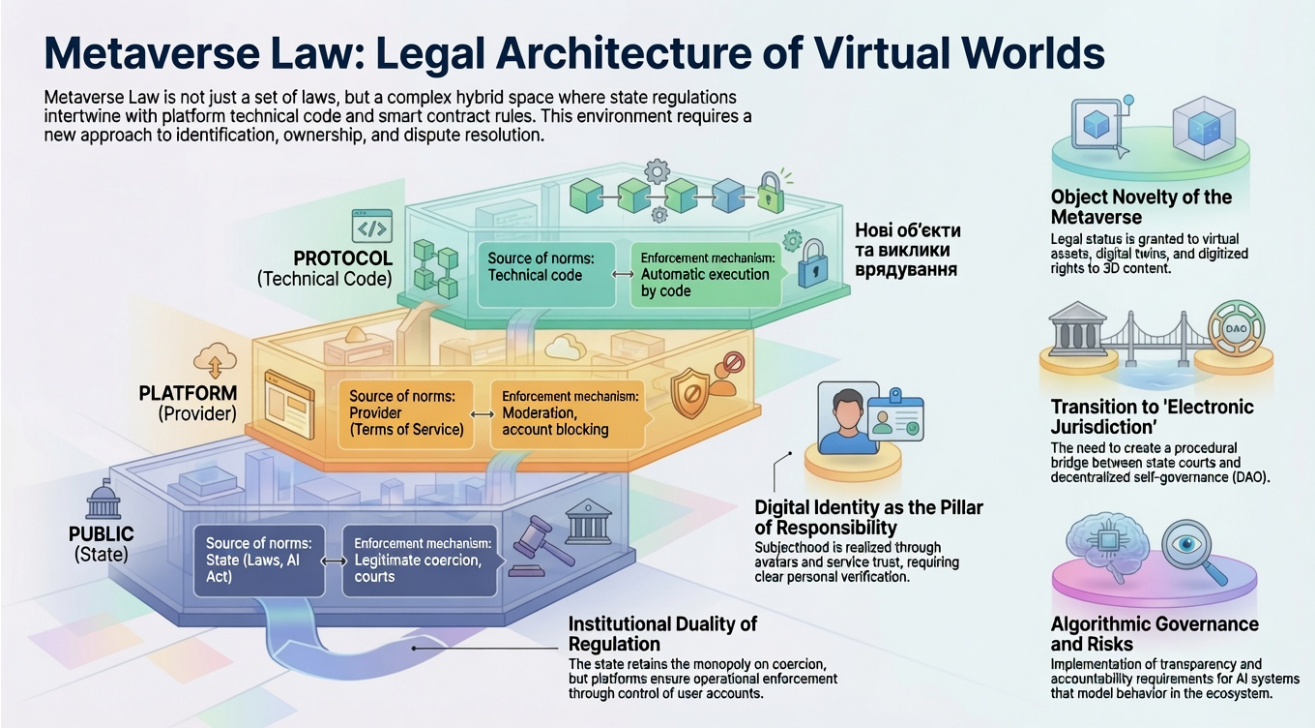


Figure 24. Metaverse as a technological-social configuration.

On this basis, Metaverse digital law should be defined as a stratified (multi-layered) regulatory and procedural complex that regulates the occurrence, change, and termination of legal relations in Metaverse environments and provides legal interoperability between the state legal order, private platform regimes, protocol rules (smart contracts, DAO charters), trust and evidentiary standards (Figure 24). Thus, the category of stratification is methodically precise, since the Metaverse functions as a "hybrid space of norms": government regulations do not disappear, but their practical implementation is often mediated by provider policies, access architecture, code and event logs, i.e. technical and legal mechanisms.

The first main feature of Metaverse law is multi-source and hybrid rule-making. Within one case, the following can simultaneously apply: imperative prescriptions of public law (data protection, cybersecurity, consumer guarantees, anti-fraud), dispositive rules of private law (contractual terms for digital goods/services), "internal rules" of platforms (Terms of Service, moderation rules), as well as protocol norms built into the technical architecture (smart contracts, tokenomics, access mechanisms) (Uçar & Taşkıran, 2023)[3].

1 Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of legal regulation web and the model of the electronic jurisdiction of the metaverse. *Bratislava Law Review, 6*(2), 21–36. https://doi.org/10.46282/blr.2022.6.2.316

2 Kostenko, O., Dniprov, O., Zhuravlov, D., Tykhomyrov, O., & Vladov, S. (2025). A new paradigm of metaverse philosophy: From anthropocentrism to metasubjectivity. *Philosophies, 10*(6), 117. https://doi.org/10.3390/philosophies1006011

3 Uçar, L., & Taşkıran, M. N. (2023). A new dimension in the digital world: An examination of the concept of Metaverse. *Journal of History School (JOHS), 16*(63), 688–701. https://doi.org/10.29228/joh.67694

The second feature is the institutional duality of regulation: the state maintains a monopoly on legitimate coercion and determines the limits of legitimacy, but the platform (or protocol) often provides "operational executability" through control of accounts, content, transactions and data.

The third feature is protocolality: a significant part of the rules in the Metaverse is implemented as technical restrictions, and not as textual prescriptions, which reinforces the requirement to "translate" protocol rules into legally controlled procedures (audit, appeal, due process).

The fourth feature is digital identity as a pillar of legal personality and responsibility. In the Metaverse, subjectivity almost always "passes" through the account, avatar, means of authentication, and associated event logs; therefore, legal regulation cannot be limited to the abstract construction of the "user" (Gupta & Pal, 2023).[1]

For the Ukrainian legal system, the Law of Ukraine "On Electronic Identification and Electronic Trust Services" can serve as a key infrastructure framework here, which sets the conceptual framework and trust regimes (in particular, tools for authentication, time fixation and confirmation of the integrity of electronic data).

This means: the binding of legally significant actions to a person in the Metaverse must be operationalised through trust services, identification/verification procedures, and evidentiary standards, otherwise the issue of liability will remain "suspended" between anonymity, pseudonymity, and platform discretion.

The fifth feature is object novelty and the need for legal ontology. In the Metaverse, not only things and services in the classical sense, but also digital assets, tokenised rights, in-platform items, digital twins, spatio-temporal data, "semantic layers" of the environment, and creative results embedded in 3D content become legally significant objects. This necessitates clear definitions: "virtual assets" as potential objects of civil circulation; "digital things/digital goods" as objects of rights and obligations; "digital twin" as a complex of data and models that can have property value and a sensitive personal dimension. At the same time, the Law of Ukraine "On Virtual Assets", as reflected in the database of the Verkhovna Rada, has the status of "not entered into force" and provides for a special procedure for entry into force (dependent on amendments to the Tax Code regarding the taxation of transactions with virtual assets) (Chai et al., 2023).[2]

The sixth feature is decentralised governance and the emergence of quasi-regulatory institutions (DAOs, protocol boards, on-chain arbitrations). In the legal plane, this gives rise to key questions: whether a DAO can be considered as an organisational form capable of being a bearer of rights and obligations; how responsibility is distributed between protocol developers, token holders, and interface operators; what minimum procedural guarantees should be built into the mechanisms of "digital self-government". In view of this, it is here that the need for a "digital" as an institutional-procedural bridge between state law enforcement and intra-protocol dispute resolution mechanisms is manifested,

1 Gupta, R., & Pal, S. K. (2023). Concept of metaverse. In *Introduction to metaverse*. Palgrave Macmillan. https://doi.org/10.1007/978-981-99-7397-2_

2 Chai, Y., Qian, J., & Younas, M. (2023). Metaverse: Concept, key technologies, and vision. *International Journal of Crowd Science, 7*(4), 149–157. https://doi.org/10.26599/IJCS.2023.910002

including requirements for due process, transparency, the ability to review and audit decisions (Safitra et al., 2023)[1].

The seventh feature is cross-border and conflict-of-laws, which makes the Metaverse a legal order of increased complexity. Relationships often have a broken link: the user is in one jurisdiction, the platform is registered in others, servers/cloud infrastructure is registered in a third, and the digital asset can circulate globally. This actualises the issues of applicable law, competent court, enforcement of judgments and access to electronic evidence. As a comparative "legal template", the UNCITRAL MLETR approach is indicative (Model Law on Electronic Transferable Records), which demonstrates how the principle of functional equivalence can provide cross-border recognition of electronic records as legally significant instruments (Karaarslan & Yazici Yilmaz, 2023)[2].

For the Metaverse, this means the need to establish standards of legal interoperability: unified requirements for the authenticity, integrity, control, and "chain" of digital evidence.

The eighth feature is algorithmic governance and a regulatory risk approach. Metaverse ecosystems widely use AI systems for moderation, personalisation, security, fraud detection, content synthesis, and even automated access and sanctions decisions. Therefore, Metaverse law must include requirements for algorithmic transparency, non-discrimination, and accountability, otherwise the "code" will effectively replace the right without proper control. The European AI Act (Regulation (EU) 2024/1689), published in the Official Journal of the EU, institutionalises the risk-based model and is a significant benchmark for benchmarking approaches to high-risk systems and prohibited practices (Zhang et al., 2022; International Telecommunication Union, 2023)[3, 4].

We assume that the Metaverse claims to be the next digital archetype of society — a comprehensive infrastructure of digital interaction capable of influencing labour, education, communication, consumption, public services, etc. (Figure 25). At the same time, the scientific literature emphasises asymmetry: positive expectations are described in much more detail than negative socio-legal implications, and some estimates are based on extrapolations from "similar" technologies without sufficient expert verification. In this regard, it is advisable to consider what has been avoided by scientists until now due to the persistent imagination of a priori "digital positivity" of electronic and digital ecosystems. It is proposed to study the concept of multidisciplinary and multi-vector reproduction of the "dark side" of the Metaverse, which allows translating disparate risks into a legally relevant plane — as a basis for the formation of legal regimes, supervision procedures and standards of evidence.

---

1 Safitra, M. F., Alhari, M. I., Putri, D. P., Lubis, M., Fakhrurroja, H., & Praditha, V. S. (2023). Metaverse trend: Definition, application, opportunities, law, and ethics. In *2023 IEEE International Conference on Computing (ICOCO).* 160–165. IEEE. https://doi.org/10.1109/ICOCO59262.2023.10397864

2 Karaarslan, E., & Yazici Yilmaz, S. (2023). Metaverse and decentralization. In F. S. Esen, H. Tinmaz, & M. Singh (Eds.), *Metaverse* (Studies in Big Data, Vol. 133). Springer. https://doi.org/10.1007/978-981-99-4641-9_3

3 Zhang, X., Chen, Y., Hu, L., & Wang, Y. (2022). The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics. *Frontiers in Psychology, 13*, 1016300. https://doi.org/10.3389/fpsyg.2022.101630.

4 International Telecommunication Union. (2023, October). *Metaverse: An analysis of definitions* (FGMV-02). ITU Focus Group on Metaverse. https://www.itu.int/en/ITU-T/focusgroups/mv/Documents/List%20of%20FG-MV%20deliverables/FGMV-02.pdf

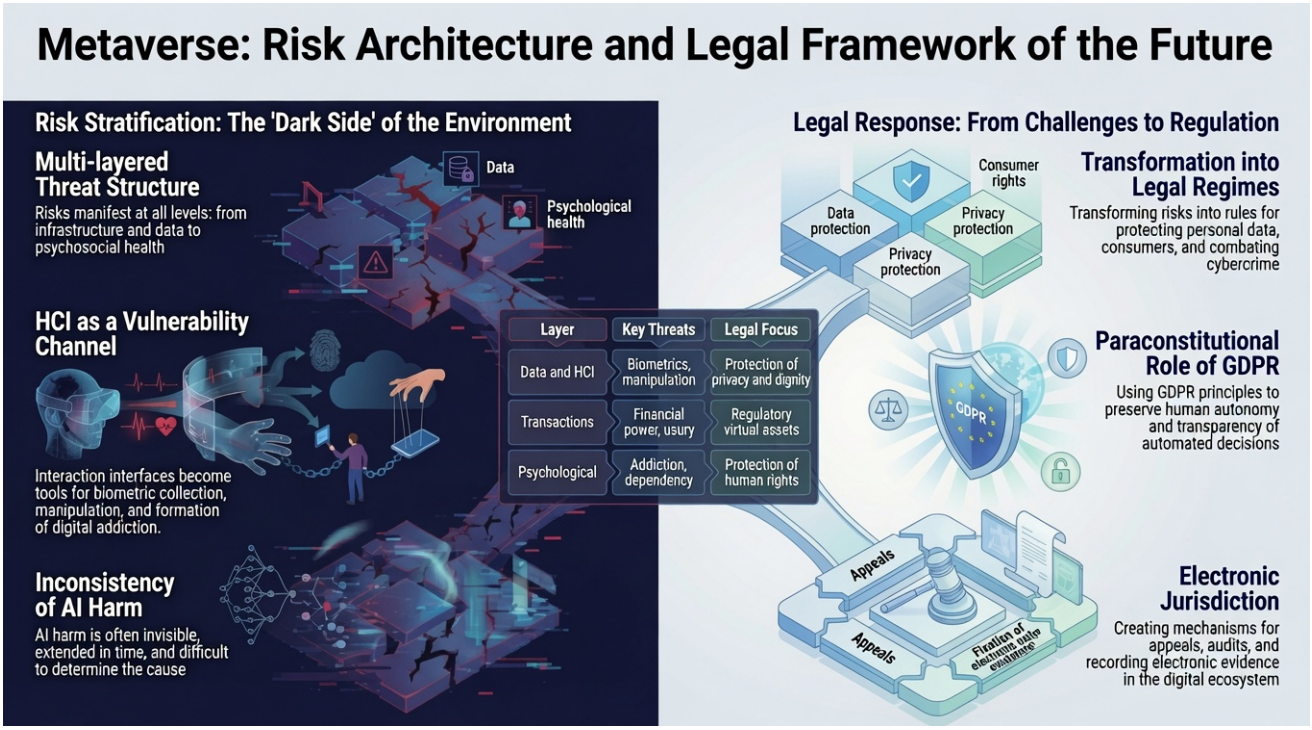


Figure 25. Metaverse as a digital archetype of society.

Within the framework of this concept, it is advisable to interpret risks as a stratified set of threats that manifest themselves on different "layers" of the Metaverse environment:

a) infrastructure (networks, devices, identification) (Wang et al., 2022; Ali et al., 2022; Pooyandeh et al., 2022)[1,2,3],

b) data and profiling (personal/biometric/behavioural data) (Huang et al., 2023; McKnight et al., 2002)[4,5],

c) content (disinformation, propaganda, manipulation) (Dwivedi et al., 2023; Gomez-Quintero et al., 2024)[6,7],

1 Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials, 25*, 319–352. https://doi.org/10.1109/COMST.2022.3202047.

2 Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2022). Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions. *IEEE Communications Surveys & Tutorials, 26*, 1238–1278. https://doi.org/10.1109/COMST.2023.334717.

3 Pooyandeh, M., Han, K., & Sohn, I. (2022). Cybersecurity in the AI-based metaverse: A survey. *Applied Sciences, 12*(24), 12993. https://doi.org/10.3390/app122412993

4 Huang, Y., Li, Y., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics, 6*, 234–247. https://doi.org/10.26599/bdma.2022.902004.

5 McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81.

6 Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., Koohang, A., Ribeiro-Navarrete, S., Belei, N., Balakrishnan, J., Basu, S., Behl, A., Davies, G. H., Dutot, V., Dwivedi, R., Evans, L., Felix, R., Foster-Fletcher, R., Giannakis, M., … Yan, M. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers.* 10400. https://doi.org/10.1007/s10796-023-10400-x

7 Gomez-Quintero, J., Johnson, S., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures, 158, Article 103338.*. https://doi.org/10.1016/j.futures.2024.103338.

d) transactional (virtual assets, fraud, financial crime) (Smaili & De Rancourt-Raymond, 2022)[1],

e) psychosocial (addiction, mental health, sexual harassment),

f) criminogenic (phishing, cybercrime, potential facilitation of terrorist activity).

Therefore, this stratification is methodologically correct, since "risk" in the Metaverse rarely has one cause: it arises at the intersection of access architecture, attention economy, recommendation algorithms, and a shortage of procedural safeguards.

These categories of "dark side" (technological and consumer vulnerabilities, privacy and "reduced reality", identity theft, invasive advertising, disinformation, propaganda, phishing, financial crimes, abuse, pornography, sexual harassment, unintended consequences) are proposed to be translated into the language of legal regimes. In particular, we are talking about the protection of personal data, the legal regime of digital identity, the protection of the rights of consumers of digital services, criminal law counteraction to cybercrimes, the regulation of advertising and unfair commercial practices, the protection of the rights of minors, as well as the procedures of digital jurisdiction (mechanisms for complaint, dispute resolution, fixation and evaluation of electronic evidence) as an institutional bridge between platform rules and state law and order.

Separately, it is necessary to actualise the issue of digital citizenship in the context of mass state, corporate and private AI, proposing a rethinking of political affiliation and inclusiveness as a legal and political category. It should be considered essential that digital citizenship is revealed not as a metaphor, but as a normative project that is based on the principles of information self-determination and data sovereignty, algorithmic participation and representation, as well as equitable distribution in the economy data; at the same time, it highlights the risks of privacy and security conflict, access barriers, digital literacy deficits, and the problem of AI accountability (Sánchez Corrales, 2024)[2]. These principles can be interpreted as "constitutional" guidelines for building the normative framework of Metaverse ecosystems, in which digital identity does not turn into a segregation tool, and algorithmic solutions do not turn into opaque "quasi-governmental" governance.

Regarding the problem of GDPR. Although the GDPR is not formally a constitutional act, in the scientific world it is interpreted as performing a paraconstitutional function, "translating" the basic values of the constitutional order into the language of an algorithmic society. Attention is focused on the rules of automated decision-making, which are designed to preserve human autonomy, increase legal certainty and provide procedural safeguards built into digital processes (Celeste & De Gregorio, 2022)[3]. This is a reason to emphasise that Metaverse regulation should require not only material prohibitions, but also procedural architecture: rights to explanations, appeal mechanisms, audits, and requirements for the traceability of decisions.

---

1 Smaili, N., & De Rancourt-Raymond, A. (2022). Metaverse: Welcome to the new fraud marketplace. *Journal of Financial Crime*. Advance online publication. https://doi.org/10.1108/JFC-06-2022-0124

2 Sánchez Corrales, C. J. (2024). *Rethinking digital citizenship: An inclusive political belonging model for the age of ubiquitous AI*. ResearchGate. https://doi.org/10.13140/RG.2.2.24006.69441

3 Celeste, E., & De Gregorio, G. (2022). Digital humanism: The constitutional message of the GDPR. *Global Privacy Law Review, 3*(1), 4–18. https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/3.1/GPLR2022002

Another scientific motive is also indicative: in the human-centric dimension, AI problems are not reduced to a list of "violated rights" (privacy, non-discrimination, freedom of expression), since AI challenges the very notion of how harm occurs, when it becomes noticeable, and to whom it is causally attributed. Three inconsistencies — notability, temporality, and causality of harm — should be singled out, which undermine the classical conditions for the effective protection of human rights in legal-positivist models (Teo, 2022)[1], that this reinforces the argument that digital jurisdiction is needed as an evidence-procedural tool that can "bring to the surface" harm through proper standards for fixing, verifying and evaluating digital traces.

A number of studies are publications describing the Metaverse as a new paradigm of digital interaction and exploring ecosystem "building blocks" (XR and related technologies), as well as their implications for companies, governments, and society. It should be noted that this is not futurology, but the basis for distinguishing legally significant contours: where new objects of circulation arise, how service delivery models change, where dependence on platforms appears, and how policy-making and enforcement challenges arise (Schmitt, 2022; Weber & Pommerin, 2023)[2,3], because the value of such sources lies in the fact that they allow you to link the "technical map" of the ecosystem with the "map of legal regimes", without substituting the law for a technological description.

Finally, a separate topic concerns the interaction of humans and technology — computers (HCI) in the Metaverse have a direct legal gateway: HCI is the "entrance" to the Metaverse, and therefore a key channel for collecting sensitive data (biometrics, motor skills, gaze, voice, behavioural patterns), the formation of dependence on interfaces, and the emergence of risks of manipulation. Human-computer interaction (HCI) emerged with the advent of the computer and has been improved over decades of development. The Metaverse has attracted significant interest due to its immersive experience, and HCI is the gateway to the Metaverse for humans. HCI is predicted to define Metaverse immersion. However, HCI technologies in the Metaverse are not mature enough. There are many problems that need to be solved for HCI in the Metaverse (Lin et al., 2023)[4]. In the legal interpretation, this means the need to establish requirements for secure interface design, data minimisation, transparency of sensory collection, procedural accountability of interaction algorithms, and standards for the protection of privacy and dignity in environments where "immersion" actually becomes a form of regulated behaviour.

1 Teo, S. A. (2022). How artificial intelligence systems challenge the conceptual foundations of the human rights legal framework. *Nordic Journal of Human Rights, 40*(1), 216–234. https://doi.org/10.1080/18918131.2022.2073078

2 Schmitt, M. (2022). *Metaverse: Implications for business, politics, and society.* SSRN. https://doi.org/10.2139/ssrn.4168458

3 Weber, D., & Pommerin, F. (2023). The metaverse and its role in social media. In A. K. Langner & G. Schuster (Eds.), *Holistische social-media-strategien.* Springer Gabler. https://doi.org/10.1007/978-3-658-42563-0_1

4 Lin, H., Gan, Z., Gan, W., Qi, Z., Wang, Y., & Yu, P. S. (2023). Interaction in metaverse: A survey. In *Proceedings of the 2023 IEEE International Conference on Big Data (BigData)* (pp. 2473–2482). IEEE. https://doi.org/10.1109/BigData59044.2023.1038687

In view of the above, it can be summarised that

First:

the main features of Metaverse law form an integral system: hybridity of sources and stratification of regulators; institutional duality "state — platform/protocol";

protocol as a technical and legal mechanism of rationing;

digital identity as a tool of legal personality and responsibility; object novelty (virtual assets, digital twins, semantic data) and the need for legal ontology;

decentralised governance (DAO) and the requirement of procedural safeguards; cross-border and conflict-of-laws

algorithmic governance and risk-based rationing.

It is this design that allows you to turn disparate descriptions of the Metaverse (including media discourses) into a legally usable toolkit for the next sections of the dissertation — in particular, for building a model of digital jurisdiction, liability regimes, and evidentiary standards in immersive digital ecosystems

Second.

The above forms an evidentiary framework for two interrelated theses:

firstly, the "dark side" of the Metaverse is not a peripheral plot, but a systemic set of risks that must be translated into the language of legal regimes;

secondly, effective legal enforcement of the Metaverse requires a stratified regulatory model with a central role of procedural safeguards, accountability, and digital jurisdiction, capable of ensuring legal interoperability between platform rules, protocol mechanisms, and government order.

Third.

The formation of the right field of digital ecosystems should begin immediately and develop models of digital jurisdiction (cross-border and national), digital codes and legislation that will regulate the rights and obligations of digital actors of the future digital society.

CHAPTER 2. TECHNOLOGICAL, ETHICAL, AND LEGAL DETERMINANTS OF THE METAVERSE.

2.1. Web 4.0 as a technological basis for the formation of legal relations in the Metaverse: theoretical and legal analysis

2.1.1. Artificial Intelligence as a Core Component of Web 4.0.

Another driver of digital social relations are artificial intelligence, artificial neural networks and machine learning, which are used by developers and researchers to optimise decision-making processes in almost all areas of human life, especially where it is possible to identify and use large statistical data. Basically, these technologies are used to create a software product that can be described as artificial intelligence of "brute force", that is, one that acts according to certain algorithms, calculating all options and calculating the most effective option for a given task with a greater probability of achieving the goal by simply iterating. Granting "autonomy" to artificial intelligence has enough risks, which consist in the inability to control the processes of self-learning in full so that a person has the opportunity to perfectly trace the entire chain of "decision-making". That is, during the process of machine learning, "black box or dark cloud" arise - data processing processes that cannot be subjected to third-party analysis (Lo Piano, 2020)[1]. In addition, at this stage of technical development, artificial intelligence is not able to recognise the significance, practical importance and feasibility of the results obtained in a statistical sample.

Attention should be paid to recent studies among artificial intelligence programs, which have revealed a feature by which artificial neural networks demonstrate a new type of system error – overinterpretation (Carter et al., 2020; Vouros, 2022)[2,, 3]These are "anti-solutions", which consist in the fact that artificial machine learning algorithms form predictions by analysing super big data, detect data that does not make sense to a person and is not related to the solution of the problem. Thus, when analysing large amounts of data, for example, a theatre of military operations in a metropolis, artificial intelligence is not able to guarantee the distinction between a civilian and a military subject or object, instead, it has the opportunity to establish that the hospital building contains a threat and needs to be destroyed.

There is also a very real threat of "input poisoning" or the introduction of "poisonous data" into deep algorithms of artificial intelligence and artificial neural networks, both at the stage of algorithm development and at the stage of data processing (Cinà et al., 2022;

1 Lo Piano, S. (2020). Ethical principles in machine learning and artificial intelligence: Cases from the field and possible ways forward. *Humanities and Social Sciences Communications, 7*, 1–7. https://doi.org/10.1057/s41599-020-0501-9.

2 Carter, B., Jain, S., Mueller, J., & Gifford, D. (2020). Overinterpretation reveals image classification model pathologies. *Proceedings of the AAAI Conference on Artificial Intelligence, 34*(07), 15395–15407. https://doi.org/10.1609/aaai.v34i07.7003.

3 Vouros, G. A. (2022). Explainable deep reinforcement learning: State of the art and challenges. *ACM Computing Surveys, 55*(5), 1–39. https://doi.org/10.1145/3527448

Paracha et al., 2024; Dunn et al., 2020)[1,2,3]. For example, if when processing information on the safety of the use of all types and types of writing pens (ink, ballpoint pens, rollers, etc.), data on a "shooting pen" (firearms disguised as a writing pen) is entered, there is a possibility that according to the overall result, all writing pens can be recognised as a military weapon, and the owner of the pen can be recognised as an armed criminal.

2.1.2. Epistemological limits of artificial intelligence.

In the legal doctrine, the starting point is not the biological or technical status of a certain "being", but its qualification as law. In this "option", everything that falls into the sphere of legal regulation is distributed according to the basic scheme: persons as bearers of legal personality and things as objects of rights. 2025; Nurmagambetov et al., 2023; Brożek & Jakubiec, 2017)[4 5,6].

Hence the key criterion: only persons can be subjects of rights and obligations in the legal sense; "non-persons" remain in the status of objects to which the powers of persons are directed. Such a construction has not only theoretical, but also applied value, since it provides certainty in the issues of attribution of actions, responsibility and application of sanctions. In other words, the legal order "works" primarily with persons as addressees, while objects are the sphere of legal domination, use or disposal.

Within the evolution of technology and science, new man-made formations — in particular, algorithmic systems, autonomous robots, hybrid digital agents — are usually primarily perceived as objects of the legal regime. Such primary "objectification" is a typical reaction of the right to innovation: until normative recognition is formed, the legal order tends to consider the new as a thing, instrument, property or, depending on the properties, as a source of increased danger or a component of a service. At the same time, according to the doctrinal approach, this status is not "eternal" — it can be changed by an act of legal recognition.

The turning point is the decision of the legislator to grant legal personality. In the tradition of legal theory, this is interpreted as a manifestation of sovereign law-making power: the legal order is able to "create" a person legally, even if such a "person" is abstract and does not have a physical nature (companies, associations, foundations). In this sense, legal personality is, first of all, a legal technology for ordering interactions — the "inclusion" of a certain entity in the circle of addressees of norms. It is emphasised

1 Cinà, A., Grosse, K., Demontis, A., Vascon, S., Zellinger, W., Moser, B., Oprea, A., Biggio, B., Pelillo, M., & Roli, F. (2022). Wild patterns reloaded: A survey of machine learning security against training data poisoning. *ACM Computing Surveys, 55*(13), 1–39. https://doi.org/10.1145/358538.

2 Paracha, A., Arshad, J., Farah, M., & Ismail, K. (2024). Deep behavioral analysis of machine learning algorithms against data poisoning. *International Journal of Information Security.* Advance online publication. https://doi.org/10.1007/s10207-024-00940-x

3 Dunn, C., Moustafa, N., & Turnbull, B. (2020). Robustness evaluations of sustainable machine learning models against data poisoning attacks in the Internet of Things. *Sustainability, 12*(16), 64-84. https://doi.org/10.3390/su12166434.

4 Inoyatov, N. (2025). Vital and Sophia robots as new legal subjects in the digital age. *Review of Law Sciences, 9(*2), 109–117. https://doi.org/10.51788/tsul.rols.2025.9.2./ugio1061

5 Nurmagambetov, R., Ukin, S., & Nalizko, N. (2023). New objects of law created by digital technologies and legal consequences of legal relations with them. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, *75*(4), 53–64. https://doi.org/10.52026/2788-5291_2023_75_4_53

6. Brożek, B., & Jakubiec, M. (2017). On the legal responsibility of autonomous machines. *Artificial Intelligence and Law, 25*(3), 293-304. https://doi.org/10.1007/s10506-017-9207-8

separately that the legislator may or may not grant certain entities the status of a "person", regardless of their "natural" nature.

Such logic opens up space for discussion about artificial intelligence as a potentially "abstract being" for which normative recognition is theoretically possible (to the extent that the legal order recognised legal entities). However, such a step requires not a metaphysical, but a functional and legal justification: what problems of legal regulation it solves, whether it increases the level of protection of victims, and whether it does not create mechanisms for "dissolving" responsibility. It is important that the second consequence of the division into subjects and objects is that only persons can be subjects of obligations (in the sense of the obligation to act/maintain and bear the legal consequences of the violation).

Artificial intelligence in applied definition appears as a system of algorithms with the property of autonomous learning, which allows you to go beyond the initially specified instructions. It is autonomisation and emergent effects of behaviour that can generate situations of harm to third parties, in which traditional liability constructs (especially those that concentrate on guilt or the predictability of a particular action) face practical difficulties. Against this background, the European discourse describes the idea of assigning AI systems the status of a "civilian" as a potential tool for solving the problem of compensation and risk sharing.

At the same time, for the correct legal argumentation, it is important to distinguish between agency in law and subjectivity in philosophy. The law can "appoint" a bearer of responsibility taking into account the goals of compensation and prevention of harm, without proving the presence of internal mental states in the person to whom the action is attributed. Therefore, legal subjectivity is able to function as a technical fiction to order interactions. However, this does not automatically imply the need to recognise AI as a "person": the complexity of the algorithm alone is not a sufficient reason to transfer the centre of responsibility from people and organisations to the technical system.

The "exceptionalism" approach (that supposedly robotics/AI "should be responsible for themselves") is assessed as theoretically unconvincing and practically risky. It mixes causality and control, and ignores that legal responsibility in modern law often fulfils economic-regulatory functions: it stimulates due diligence, proper design, auditing, quality control, insurance and compliance. With this logic, it is more reasonable to focus on the entities that organise risky activities and benefit from them: developers, integrators, suppliers, operators, customers, and in the public sphere — on the state as guarantors of good administration and human rights.

As a result, a restrained doctrinal position is proposed, which does not duplicate the general considerations of the previous sections: the recognition of the legal personality of AI can be considered only as a special regulatory and technical tool and only if it really strengthens the protection of victims and does not replace the personified responsibility of people and organisations. On the other hand, in most application scenarios (including Metaverse environments with digital identity and protocol management), a different legal design seems to be a priority: a clear definition of responsible persons, mandatory traceability and audit procedures, risk-sharing rules, and a guaranteed effective remedy for victims.

Artificial intelligence is not an automaton that will completely replace a person and perform all his work, including the exclusively intelligent, software part of the created automated system, in which the routine part is performed by the automaton, and the creative part remains with the person.

2.1.3. Robotics, AI: responsibility and legal personality

In view of the development of science and technology, "new beings" (including artificial intelligence systems and autonomous robots) first appear as objects in legal thinking. Such an entity, which society perceives, knows and accepts as an object, remains an object until the legal order declares it a "person". In doctrine, this "act of giving personality" is interpreted as a sovereign (law-making) decision of the legislator, is able to extend legal individualisation even to abstract entities (for example, legal entities — companies, associations, foundations) that do not have a physical body, but act as bearers of rights and obligations. In this sense, legal personality is not reduced to natural qualities, but is a legal construction that "turns on" the mode of addressability of the norm for the essence (Alabdulkarim, 2023)[1].

A key dilemma arises for the right of AI: whether there are grounds to recognise artificial intelligence (as an abstract, protocol-algorithmic entity) as a person, or whether it is more correct to preserve the object status with an enhanced regime of responsibility of people and organisations that design, implement, and control such systems. On the one hand, the legal order is able to "construct" subjectivity in order to facilitate legal interactions; on the other hand, a legal entity should not become an escape tool from liability or blurring of the chain of attribution of damages. That is why the issue of recognising AI as a "person" should be considered not as a metaphysical, but as a purely normative and functional one: what tasks of legal regulation does it solve and what risks does it pose (Da Anunciação Melo & Ribeiro Cardoso, 2022)[2].

Artificial intelligence in the modern applied sense can be defined as a system of algorithms, the characteristic property of which is the ability to learn autonomously, which allows the machine to go beyond the initially programmed scenarios. Autonomy, combined with emergent behaviour, creates situations of harm to third parties, in which the classical constructions of civil (and sometimes criminal) liability face complications due to their attachment to guilt or to the human controllability of the action. In this plane, there is a discussion about the possibility of assigning AI systems the status of a "civilian" as a technical solution for redistributing risks and providing compensation for damages, including a hypothetical-deductive analysis of such approaches in the European discourse.

Methodologically, it is important to distinguish the legal agency (the ability to be the addressee of the prescription and the bearer of the duty) from the ontological subjectivity (the presence of an "internal" intention or conscious experience). In law, responsibility is primarily an instrument of compensation and restraint (ex ante and ex post), and not a moral assessment of the internal state of the "culprit". Therefore, the constructions of legal subjectivity can be purely "fictitious" and technical, aimed at facilitating legal interactions, and do not depend on the nature of internal processes in a robotic or algorithmic system. This allows us to form a discussion about the feasibility of the legal

1Alabdulkarim, A. (2023). *Legal personality of artificial intelligence.* ResearchGate. https://www.researchgate.net/publication/367207390_Legal_Personality_of_Artificial_Intelligence

2 Da Anunciação Melo, B. L., & Ribeiro Cardoso, H. (2022). Artificial intelligence systems and civil liability: An analysis of the European proposal on the attribution of civil personality. *Brazilian Journal of Fundamental Rights & Justice, 16*(1). https://doi.org/10.30899/dfj.v16i1.1318

personality of AI without substituting a legal issue for a philosophical dispute about the "consciousness" of machines (Bertolini & Episcopo, 2022)[1].

At the same time, the author does not share the "claim of exclusivity", according to which robotics and AI are so technologically advanced that they "should" be responsible for their actions, and not the people who develop or apply them. This approach is theoretically erroneous and practically inadequate, since it mixes:

1) the issue of causality (what caused the damage),

2) the issue of control (who had the opportunity to prevent),

3) the issue of risk distribution (who will economically benefit from the technology), and

4) the issue of evidence (who is able to explain and check the operation of the system).

If legal responsibility performs the functions of compensation and prevention, then its focus should remain on the entities that organise risky activities: manufacturers, integrators, operators, customers, and in the public sphere — on the state as a guarantee of human rights and good administration.

In view of the above, in the further logic of the dissertation research, a working position is proposed: the legal personality of AI can only be considered as an exceptional regulatory and technical construction, permissible when it increases the level of legal protection of victims and does not weaken the personification of the responsibility of people and organisations. On the other hand, in most practical scenarios (in particular, in Metaverse environments where AI interacts with digital identity, virtual assets, and protocol rules), the following regime seems to be more productive: a) clear identification of responsible persons, b) audit procedures and traceability of decisions, c) special rules for risk distribution, d) guaranteed legal remedies for victims. It is this construction that is consistent with the functions of the right of responsibility as a mechanism of compensation and deterrence, and not as a "recognition of the dignity" of the technical essence.

2.1.4. Human Rights, Ethics, and Social Effects of AI

Few recent developments have captured the human imagination as much as those related to artificial intelligence. The increasing prevalence and ubiquity of AI are impacting both the lives of individuals and society as a whole. However, human rights concerns that have arisen in connection with artificial intelligence are focused primarily around violations of these individual rights, such as privacy, non-discrimination, and freedom of expression and information. While it is important to study individual rights that are at risk, there is a fundamental gap between human rights and artificial intelligence at a fundamental level, as AI systems increasingly challenge ideas about how, by whom, and what human rights are violated. The legal-positivist registration of individual rights themselves is considered through the analysis of the inconsistent typology of harm between the objects of human rights protection and the threats created by AI systems.

These and other studies have become the basis for accelerating the improvement of the legislative framework governing legal relations in the field of robotics. Thus, the

1 Bertolini, A., & Episcopo, F. (2022). Robots and AI as legal subjects? Disentangling the ontological and functional perspective. *Frontiers in Robotics and AI, 9*, 842213. https://doi.org/10.3389/frobt.2022.8422

European Parliamentary Research Service (EPRS) and the European Parliament's Legal Affairs Committee are developing recommendations on improving the civil and ethical aspects of robotics, which propose to create a register of robots and the corresponding EU Agency for Robotics, as well as to establish civil liability for damage caused by robots in accordance with and in proportion to the actual level of instructions given according to the degree of its autonomy. At the same time, it is planned to entrust the Agency with the task of carrying out technical, ethical and regulatory expertise in the field of robotics and developing the "Code of Ethical Conduct for Robotics Engineers" and the "Code of Research Ethics Committees". The "Code of Ethical Conduct for Robotics Engineers" is proposed to be developed on the basis of the following ethical principles of robotics:

1) good (robots must act in the interests of people);

2) not harmfulness (robots should not harm people);

3) autonomy (human interaction with robots must be voluntary);

4) equity (the benefits of robotics should be distributed fairly) (European Parliament Research Service, 2017)[1].

Google presents a "white paper on artificial intelligence" (Perspectives on Issues in AI Governance), which highlights the general problems of using artificial intelligence at the conceptual level (Google, 2019)[2].

At the end of 2021, 193 UNESCO member countries adopted a document defining the common values and principles necessary to ensure the safe development and use of artificial intelligence. The document adopted by UNESCO member states is aimed at creating a legal infrastructure to ensure the ethical development of artificial intelligence technology. UNESCO has facts that indicate the use of artificial intelligence by individual governments in decision-making. UNESCO warns that this technology has the potential to create "unprecedented problems".

"We are witnessing manifestations of gender and ethnic prejudice, as well as violations of privacy and freedoms, the danger of mass surveillance and the abuse of artificial intelligence technology by law enforcement agencies, until recently there were no universal standards capable of limiting such abuses" (UNESCO, 2020).[3] The adopted document establishes the world's first global regulatory framework and holds states responsible for its application and lays the foundations for digital jurisdiction.

2.1.5. Military AI.

Immersion and Metaverse technologies are being integrated into the military sphere no less intensively, forming a new category of socially dangerous risks that require not only technical, but primarily legal regulation. We are talking about the convergence of XR simulators, digital twins, network-centric control systems, autonomous platforms, and algorithmic decision support. In the legal dimension, this means a shift from the classical model of "weapons as a material object" to the model of "weapons as a cyber-

1 European Parliament Research Service. (2017). *Civil law rules on robotics.* https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599250/EPRS_ATA(2017)599250_EN.pdf

2 Google. (2019). *Perspectives on issues in AI governance.* https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf

3 UNESCO. (2020). *First draft of the recommendation on the ethics of artificial intelligence (SHS/BIO/AHEG-AI/2020/4 REV.2).* https://unesdoc.unesco.org/ark:/48223/pf0000373434

physical system", where legal assessment covers data, software, communication channels, interaction protocols and human application procedures.

To preserve the terminological discipline, it is advisable to distinguish:

a) human reinforcement systems (exoskeletons, sensory complexes, integrated life support systems),

b) robotic platforms of the land/sea/air domains,

c) space communication and navigation groups,

d) brain-computer interfaces as an experimental class of controls,

e) algorithmic battle control systems.

The legal consequences of these directions differ depending on the degree of autonomy. An illustrative approach is recorded in DoD Directive 3000.09 (USA), where autonomy in weapons systems is described through the ability of the system, after activation, to independently select and hit targets without further intervention of the operator, as well as through man-in-loop/on-the-loop modes as tools to reduce the risk of unintentional damage.

In research and development dimensions (without reference to advertising images), these areas can be legally correctly outlined as follows:

firstly, the development of military personnel equipment complexes (sensorics, protection, communication, medical monitoring) as an "individualised cyber-physical system" that accumulates personal and tactical data;

secondly, the creation of robotic units and group scenarios for the interaction of unmanned platforms (swarming logic), where the problem of command, control and legal attribution of the results of actions becomes key;

thirdly, the deployment of "proliferated" low-orbit satellite constellations as a communication/surveillance/navigation component (in the United States, in particular, DARPA Blackjack programs with Mandrake 2 demonstrators and SDA architecture known as Proliferated Warfighter Space Architecture are recorded).

fourthly, experiments with non-invasive control interfaces and "human-machine command" as a direction that changes the perception of the subject of weapon control (here it is appropriate to talk about experimental trajectories, and not about established combat practices).

The legal core of the risks is that the autonomisation and algorithmisation of combat functions increases the threat of violation of the fundamental principles of international humanitarian law (distinction, proportionality, precautions), as well as complicates the chain of responsibility between the developer, integrator, commander and operator. That is why in the doctrine and practice of international law, a key safeguard is a legal review of new types of weapons, means and methods of warfare in accordance with Article 36 of Additional Protocol I of 1977, which imposes an obligation on states to determine whether the use of such a means is prohibited under international law in certain or all circumstances. Practical guidelines and algorithms for implementing this obligation are detailed by the ICRC in a dedicated guide and analyses.

The risk of "data and context" requires special attention. For military tasks, the deficit of representative training data, domain drift (a sharp change in conditions), as well as the unpredictability of "edge cases", which makes errors not a statistical abstraction, but an operational factor, are typical. In the legal plane, this translates into issues of due

diligence, standards of testing, certification and procedural accountability: if the system makes decisions in conditions of uncertainty, then the requirements for documenting the grounds, for the verifiability of models and for the presence of a stop/cancel mechanism (override) increase. — In our opinion, this is where the line between permissible "decision support" and the actual transfer of responsibility from a person to an opaque algorithm passes, which is conceptually incompatible with the requirement of personalised command and control.

The experience of the "military danger of the past" demonstrates that even high-tech surveillance and warning systems are prone to interpretation errors and false positives, and therefore require multi-level verification procedures. Thus, on December 7, 1941, a radar warning on Oahu about a large group of aircraft was mistakenly assessed as an expected "friendly" flight, which led to the failure to take proper precautions. On September 26, 1983, the Soviet early warning system "Oko" generated a signal about the "launch of missiles", which later turned out to be false, and the crisis was stopped thanks to a human assessment of the unreliability of the signal. On January 25, 1995, the launch of the Norwegian Black Brant XII scientific rocket was interpreted as a potential Trident launch, causing a short-term increase in nuclear readiness. These cases are not a "one-to-one analogy" to modern AI, but they are legally important as proof that the combination of technical signal and human error can create unacceptable escalation risks.

The problem of Internet of Things AI (AI-IoT) in military systems is a problem of cyber resilience and access control, not just "technical insecurity". When sensors and actuators are part of the force-use circuit, their compromise potentially means unlawful interference with weapon control, telemetry tampering, distortion of intelligence data, or unauthorised activation of functions. In the legal plane, this raises the issue of the state's obligation to ensure proper organisational and technical security measures, establish role-based access, multi-factor authentication, logging administrators' actions and incident response standards. A separate dimension is the identification of persons who have the right to operate robotic systems: without clear verification and logging procedures, the control entity "dissolves", and with it becomes more difficult to establish responsibility.

In view of the above, the legally balanced "ordering" of military Metaverse technologies should be based not on a list of gadgets, but on a system of regulatory safeguards:

1) mandatory reviews under Article 36 and internal procedures for certification of autonomous functions;

2) the requirement of "human control" in critical decisions regarding damage;

3) evidentiary standards for telemetry and logs (so that decisions and events are ex post verifiable);

4) cyber resilience as a legal condition for admission to operation;

5) delimitation of responsibility between the developer, integrator and command through contracts, technical protocols and service regulations;

6) supervisory mechanisms and auditing of algorithms and data.

In our opinion, without such a "procedural shell", autonomy will inevitably increase the zone of legal uncertainty and the risk of disproportionate harm. Military applications of immersion technologies are the most "demanding" testing ground for Metaverse law, as here technical innovations directly affect the right to life, humanitarian law standards,

and international liability regimes legality, accountability, and evidence, can ensure the manageability of the technological evolution of military AI in the face of high stakes (Kostenko, 2021c)[1].

2.1.6. Regulation of AI through the prism of international human rights law.

We proceed from the fact that the rapid introduction of artificial intelligence systems in public administration and the private sector actualises not only the issue of technological efficiency, but primarily the issue of legal legitimacy and compliance with the standards of international human rights law (hereinafter referred to as the ICHR). Early (proactive) regulation of AI is an element of the state's proper fulfilment of its positive human rights obligations, while the wait-and-see policy can be qualified as improper fulfilment of such obligations under certain conditions. This approach corresponds to the academic position formulated in works that directly raise the question: does the state have the right to "wait" when the risks to human rights are already predictable and systemic.

The normative basis for such a statement is the generally recognised triune construction of the state's international obligations: to respect (not to interfere unduly), to protect (prevent violations by third parties, in particular corporations) and to ensure/enforce (create institutional and procedural guarantees for the implementation of rights), as well as the obligation to provide an effective remedy in case of violation. In the field of AI, this means that the state cannot limit itself to moral guidelines or "ethical principles", if algorithmic systems are actually involved in the distribution of benefits, in decision-making regarding access to services, in the profiling of persons or in the moderation of the information space. In such a situation, the legal regime should act as a safeguard against the transformation of technological discretion into a "de facto power decision" without due process (Kostenko, 2025b)[2].

The question of temporality is critical: can "waiting" be considered a neutral position. It must be assumed that there is no neutrality here, since the regulatory pause actually allows scaling up practices that can cause discrimination, unjustified interference with privacy, restriction of access to social services or non-transparent sanctions, and therefore accumulate damage before procedural barriers are created. It is this logic that underlies an approach that denies the "reasonable" or "legitimate" nature of the wait-and-see model, when the risks to human rights are already sufficiently predictable and confirmed by empirical observations.

Legally, early regulation of AI should be understood not as an "excessive legislative burden", but as the institutionalisation of a minimum set of due diligence guarantees of the state:

1) mandatory assessment of human rights risks before the implementation of AI systems in sensitive areas;

---

1 Kostenko, O. V. (2021). Identyfikatsiia IoT: vytoky problemy pravovoho rehuliuvannia upravlinnia identyfikatsiinymy danymy [Identification of IoT: Origins of the problem of legal regulation of identification data management]. *Juris Europensis Scientia, 1,* 77–83. https://doi.org/10.32837/chern.v0i1.177

2 Kostenko, O. (2025). AI law model for ethical legislation: Strategic recommendations for the regulation of artificial intelligence. *SciFormat Publishing*. https://doi.org/10.69635/978-1-0690482-5-7

2) requirements for transparency and explainability within the limits sufficient for appeal;

3) prohibition or severe restriction of practices that are incompatible with human rights;

4) effective review procedures (appeal/complaint) and access to reimbursement;

5) supervision and audit (including independent) as a procedural condition of trust.

The use of the logic of "built-in procedural" in this context is appropriate in the context: the legal requirement should be reflected in the architecture of the process (design and deployment cycles), and not exist only in the form of a declaration.

To demonstrate that AI risks are not an abstraction, but a structural threat, we will apply a gender-oriented human rights vision (women's rights as a specific "indicator" of systemic destruction). This approach is methodically justified, since the discriminatory effects of algorithms often have the character of indirect discrimination: formally neutral criteria in practice reproduce historical inequalities in access to credit, labour, medical services, social support and security. Accordingly, the "three examples" of AI applications outlined in the human rights literature should be interpreted as model cases that reveal that the risks relate not only to privacy, but also to equality, dignity and an effective remedy, i.e. the core of the IPHR.

The fundamental thesis is that the lack of proper regulation in the field of AI can be considered as an independent legally significant fact of the state's failure to fulfil its positive obligations to protect, enforce, and remediate. In other words, a violation can be not only "incorrect application of the algorithm", but also structural regulatory inaction, which leaves a person without procedural guarantees — without the opportunity to understand the grounds for the decision, without a real appeal procedure, without access to compensation. This construction is especially evident in areas where the state or its contractors use AI to make decisions about a person's legal status or access to socially significant benefits. At the same time, a practical limitation should be taken into account: the likelihood of rapid comprehensive regulatory reforms is not always high. Therefore, within the framework of an interim (but legally effective) solution, it is right to support the approach according to which the international human rights monitoring system should require states to systematically assess and report on their readiness to manage AI risks. This does not replace regulation, but creates an accountability regime that limits the "regulatory pause", contributes to the accumulation of data on harms and allows you to identify long-term needs of legal regulation. This idea is explicitly formulated in scientific papers on the "ponderal state" (hesitant state) and is supported by the general logic of UN human rights documents in the context of digital technologies and state practices (in particular, procurement and implementation).

It should be considered appropriate to fix the minimum "procedural standard of readiness" of the state for AI risks in the human rights plane:

1) the availability of a methodology for assessing the impact on human rights (HRIA/FRIA-logic);

2) a designated competent authority or interagency coordination;

3) incident response regulations and reimbursement mechanism;

4) rules of transparency, access to information and the right to appeal;

5) special fuses for vulnerable groups.

Thus, the early regulation of AI in the coordinates of the IPHR is not a manifestation of excessive control, but a way for the state to fulfil positive obligations: to prevent harm, to ensure equality and non-discrimination, to guarantee due process and an effective remedy. that it leaves risks unmanageable and a person's legal position procedurally unprotected (Bello y Villarino & Vijeyarasa, 2022)[1].

2.1.7. Artificial intelligence strategies.

Over the past decade, many states have recognised that their future success will depend on Big Data processing and AI capabilities. Significant funds are already being invested in this area. Many private and public companies, research laboratories and scientific institutions go through the typical path of developing and creating products with artificial intelligence. First, they form their own intellectual resources for the accelerated receipt of the final result of a research or business task. As a rule, the results obtained by such a separate team for the development of artificial intelligence do not achieve a global goal or their use is narrow-profiled. In the future, the development team enters the so-called "ice age", during which either the project closes or adapts very slowly to new tasks.

It quickly became clear that local advances in the creation of AI technologies do not have a long-term scientific and technological perspective. Only a global, comprehensive, state approach has greater opportunities for the development of modern technologies.

That is why there is a need to form state strategies for managing big data and processing them through the development and application of artificial intelligence technologies. As we can see from the analysis of the annual reports of Stanford University "Artificial Intelligence Index Report", in recent years, many states have developed long-term national strategies for the development of artificial intelligence and are taking certain measures to implement them (Stanford Institute for Human-Centered Artificial Intelligence, 2021; Stanford Institute for Human-Centered Artificial Intelligence, 2022)[2,3].

In general, AI development strategies can be divided into three main groups:

A group that is distinguished by a realistic attitude to the formation of AI strategies, an in-depth analysis of not only the state of the field of artificial intelligence in the country, but also the real needs of its development. The strategies are characterised by the detailing of the plans and tasks of each stage, as well as tasks for state bodies and scientific institutions regarding the control points for the implementation of the assigned tasks.

A group of countries characterised by a thorough and rather pragmatic approach to the goals and stages of their achievement, taking into account the real needs of the state and the formation of individual unique tasks and goals for the development of AI.

This group includes countries whose strategies are implemented in a formalised form, have the basic goals of the country's development in the direction of introducing AI technologies in certain areas of social activity.

---

1 Bello y Villarino, J.-M., & Vijeyarasa, R. (2022). International human rights, artificial intelligence, and the challenge for the pondering state: Time to regulate? *Nordic Journal of Human Rights, 40*(1), 194–215. https://doi.org/10.1080/18918131.2022.2069919

2 Stanford Institute for Human-Centered Artificial Intelligence. (2021). *Artificial intelligence index report 2021.* https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.p

3 Stanford Institute for Human-Centered Artificial Intelligence. (2022). *Artificial intelligence index report 2022.* https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.p

The strategies of the countries of group "C" are mainly declarative in nature, namely: to become one of the most developed digital societies in the world; create a sustainable AI-driven economy; provide support for the development of human-centred artificial intelligence; to develop research and innovation activities focused on regulating the framework for the use of data for AI; to ensure the formation of an attractive and modern environment with artificial intelligence controls; have achievements in some perspective of regional or global leadership in the application of AI in order to improve education and form more AI specialists; implement AI technologies in logistics, general ecology, urban ecosystem, partly in medicine (gerontology) and speech and facial recognition technologies.

It is advisable to include the strategies of such states as Australia (CSIRO Data61, 2019)[1], the Republic of Austria (Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology, 2021)[2], the Republic of Bulgaria (Fondatsiya "LIBRe", 2020; Ministerski savet na Republika Balgariya, 2019)[3,4], Ministry[5] of Research [6]and Technology/National Agency for Research and Innovation of the Republic of Indonesia, 2020[7], Government of Spain (2020), 8Law Society of Ireland, 2021 (Department of Enterprise, Trade and Employment, 2021)[9], State of Qatar (Ministry of Transport and Communications, 2019),[10] Portugal (Government of Portugal, 2019)[11], Republic of Cyprus (Republic of Cyprus, 2020[12,13]), Republic of Kenya (The Kenyan

1 CSIRO Data61. (2019). *Artificial intelligence: Australia's ethics framework and roadmap.* https://data61.csiro.au/~/media/D61/AI-Roadmap-assets/19-00346_DATA61_REPORT_AI-Roadmap_WEB_191111.pdf

2 Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology. (2021). *AIM AT 2030: Artificial intelligence mission Austria 2030—Shaping the future of artificial intelligence in Austria.* https://www.bmk.gv.at/dam/jcr:8acef058-7167-4335-880e-9fa341b723c8/aimat_ua.pdf

3 Fondatsiya "LIBRe". (2020). *Stanovishte ot Fondatsiya "LIBRe" po kontseptsiya za razvitieto na izkustveniya intelekt v Balgariya do 2030 g.* [Statement of the LIBRe Foundation on the concept for the development of artificial intelligence in Bulgaria until 2030]. http://libreresearchgroup.org/p/1/3/139-2020-09-17-libre-statement-ai-strategy-bg-1136.pdf

4 Ministerski savet na Republika Balgariya. (2019). *Proekt na kontseptsiya za razvitieto na izkustveniya intelekt v Balgariya do 2030 g.* [Draft concept for the development of artificial intelligence in Bulgaria until 2030]. https://strategy.bg/FileHandler.ashx?fileId=21904

5 Ministry of Information and Communications of Vietnam. (2021). *Selecting appropriate artificial intelligence development strategy.* https://english.mic.gov.vn/Pages/TinTuc/139578/Selecting-appropriate-artificial-intelligence-development-strategy.html

6 Ministry of Research and Technology/National Agency for Research and Innovation of the Republic of Indonesia. (2020). *Strategi nasional kecerdasan artifisial Indonesia 2020–2045* [National strategy for artificial intelligence Indonesia 2020–2045]. https://ai-innovation.id/server/static/ebook/stranas-ka.pdf

7 Government of Spain. (2020). *Estrategia nacional de inteligencia artificial* [National strategy for artificial intelligence]. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/021220-ENIA.p

8 Law Society of Ireland. (2021). *Artificial intelligence consultation.* https://www.lawsociety.ie/globalassets/documents/committees/technology/artificial-intelligence-consultation.p

9 Department of Enterprise, Trade and Employment (Ireland). (2021). *Public consultation on the development of a national strategy on artificial intelligence.* https://enterprise.gov.ie/en/Consultations/Public-Consultation-Development-of-a-National-Strategy-on-Artificial-Intelligence.htm

10 Ministry of Transport and Communications (Qatar). (2019). *Blueprint: National artificial intelligence strategy for Qatar.* https://www.motc.gov.qa/sites/default/files/national_ai_strategy_-_english_0.pd

11 Government of Portugal. (2019). *AI Portugal 2030: Portuguese national initiative on digital skills—An innovation and growth strategy to foster artificial intelligence in Portugal in the European context.* https://www.incode2030.gov.pt/sites/default/files/julho_incode_brochura.pdf).

12 Republic of Cyprus, Deputy Ministry of Research, Innovation and Digital Policy. (2020). *Ethniki stratigiki technitis noimosynis: Draseis gia tin axiopoiisi kai anaptyxi tis technitis noimosynis stin Kypro* [National artificial intelligence strategy: Actions for the utilization and development of AI in Cyprus]. https://researchinnovation.gov.cy/wp-content/uploads/2020/11/AI-Strategy-Cyprus.pdf)

13 Republic of Cyprus, Deputy Ministry of Research, Innovation and Digital Policy. (2020). *National strategy for artificial intelligence.* https://knowledge4policy.ec.europa.eu/sites/default/files/cyprus_ai_strategy.pdf.

Wall Street, 2018),[1] New Zealand (Ministry of Business, Innovation and Employment, 2019), [2] Republic of Tunisia (Agence Nationale de Promotion de la Recherche Scientifique, 2018)[3], Hungary (Ministry for Innovation and Technology, 2020)[4], Israel (Calcalist Tech, 2020)[5], the Republic of Chile (Government of Chile, 2018)[6], the Swiss Confederation (State Secretariat for Education, Research and Innovation, 2020a; State Secretariat for Education, Research and Innovation, 2020; State Secretariat for Education, Research and Innovation, n.d.)[7,8,9], the Republic of Finland (State Secretariat for Education, Research and Innovation, 2019)[10].

The strategies of the countries of group "B" are characterised by a more thorough approach to the formation of national strategies for the development of AI. The strategies provide an analysis of global trends in the development of AI, an overview of the state of existing opportunities, and real achievements of the state in the field of AI application. It should be noted that the countries of this group have a rather pragmatic approach to the goals and stages of their achievement, taking into account the actual needs of the state. Thus, in addition to the general directions of AI development, the strategy lays down the goal of concentrating certain policies related to artificial intelligence, aimed at regulating the interaction of society with artificial intelligence systems; warning about the harm that AI can cause; equity in the development, deployment, use and operation of AI systems; the ability for end-users and other members of the public to challenge any operation of AI systems for each specific use case. The countries of this group include the Grand Duchy of Luxembourg, the Republic of Malta, Malaysia, and the Republic of Lithuania.

For example, the Grand Duchy of Luxembourg, proposed the creation of a regional cluster of advanced AI research, since Luxembourg is in close geographical proximity to a number of European AI research centres, such as the Research Center of the University of Lorraine (Inria Nancy-Grand Est) and its branch in Strasbourg, which is developing

1 The Kenyan Wall Street. (2018). *Kenya government sets up blockchain & artificial intelligence taskforce.* https://kenyanwallstreet.com/kenya-govt-sets-blockchain-artificial-intelligence-taskforce/

2 Ministry of Business, Innovation and Employment (New Zealand). (2019). *Artificial intelligence: Shaping a future New Zealand.* https://www.mbie.govt.nz/dmsdocument/5754-artificial-intelligence-shaping-a-future-new-zealand-pdf

3 Agence Nationale de Promotion de la Recherche Scientifique (Tunisia). (2018). *National artificial intelligence strategy: Unlocking Tunisia's capabilities potential.* http://www.anpr.tn/national-ai-strategy-unlocking-tunisias-capabilities-potential/

4 Ministry for Innovation and Technology (Hungary). (2020). *Hungary's artificial intelligence strategy 2020–2030.* https://ai-hungary.com/api/v1/companies/15/files/138309/view

5 Calcalist Tech. (2020). *Israel launches national AI program, but lack of budget threatens its implementation.* https://www.calcalistech.com/ctech/articles/0,7340,L-3883355,00.html

6 Government of Chile. (2018). *The government announces an artificial intelligence plan to be developed by the science ministry.* https://www.gob.cl/en/news/government-announces-artificial-intelligence-plan-be-developed-science-ministry

7 State Secretariat for Education, Research and Innovation (Switzerland). (2020). *"Artificial Intelligence" – Adoption of Guidelines for the Federal Administration*. https://www.sbfi.admin.ch/sbfi/fr/home/actualite/communiques-de-presse/test-bit.msg-id-81319.html

8 State Secretariat for Education, Research and Innovation (Switzerland). (2020). *Artificial Intelligence – Guidelines for the Confederation* https://www.sbfi.admin.ch/dam/sbfi/fr/dokumente/2020/11/leitlinie_ki.pdf.download.pdf/Leitlinien%20K%C3%BCnstliche%20Intelligenz%20-%20FR

9 State Secretariat for Education, Research and Innovation (Switzerland). (n.d.). *Intelligence artificial.* https://www.sbfi.admin.ch/sbfi/fr/home/politique-fri/fri-2021-2024/themes-transversaux/numerisation-fri/intelligence-artificielle.html

10 State Secretariat for Education, Research and Innovation (Switzerland). (2019). *Report of the Project Group "International Committees and Artificial Intelligence/* https://www.sbfi.admin.ch/dam/sbfi/fr/dokumente/2019/12/i-g_k-i.pdf.download.pdf/i-g_ki_d.pdf

together with the University of Strasbourg, the German Research Center for Artificial Intelligence (GmbH Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), which has offices in Kaiserslautern, Saarbrücken, Bremen, laboratories in Berlin and Lower Saxony and branches in Lübeck and Trier, as well as the Association of German Helmholtz Research Centers (Helmholtz-Gemeinschaft Deutscher Forschungszentren). In fact, Luxembourg is initiating the creation of a large-scale joint research cluster for the study of AI and data protection (Government of Luxembourg, 2019)[1].

The Republic of Malta is concentrating its efforts in the field of AI application, in the direction of creating a technical and legislative framework for artificial intelligence and the creation of a national launch pad "Ultimate AI Launchpad". Malta is establishing a National Committee on Technology Ethics to oversee ethical AI and constantly monitor the regulatory mechanisms of innovation ecosystems. Malta also plans to take the world lead in the development of regulations and a voluntary certification system Innovative Technologies in collaboration with the Institute for Technology Assessment and Systems Analysis (ITAS) (Government of Malta, 2019; Malta College of Arts, Science and Technology, 2020)[2, 3].

The Malaysian government intends to establish a regional centre for big data analysis (BDA) in the ASEAN region. Malaysia has begun work on the creation of the National Artificial Intelligence System, as part of the National Big Data Analysis System (BDA), which will be led by the Malaysian Digital Economy Corporation (MDEC). The government of the country is creating the Digital Transformation Acceleration Program (D-TAP) for large and medium-sized companies, which provide 64 percent of the gross domestic product, to accelerate the adoption of digital technologies(OpenGov Asia, 2020)[4].

The experience of the Republic of Lithuania is interesting because the country has a private sector, which has long been a leader in the introduction of innovative technologies. The implementation of public-private partnerships in the field of AI application has made it possible to implement several successful projects focused on the public, namely:

- crime forecast: AI models can be used to identify high-risk crime areas in cities;
- improve services for citizens: intelligent virtual assistants to better serve citizens;
- for government agencies: internal workflow is optimised using intelligent systems;

"regulatory sandbox" that allows the use and testing of AI systems in the public sector for a limited time in order to test AI products in a real environment and decide on the possibility of their integration in the public sector (Ministry of the Economy and Innovation of the Republic of Lithuania, 2019)[5].

---

1 Government of Luxembourg, Ministry for Digitalisation. (2019). *Artificial intelligence: A strategic vision for Luxembourg.* https://gouvernement.lu/dam-assets/fr/publications/rapport-etude-analyse/minist-digitalisation/Artificial-Intelligence-a-strategic-vision-for-Luxembourg.pdf

2 Government of Malta, Ministry for the Economy, Investment and Small Businesses. (2019). *Malta: The ultimate AI launchpad—A strategy and vision for artificial intelligence in Malta 2030.* https://economy.gov.mt/en/Documents/MaltaTheUltimateAILaunchpad.pdf

3 Malta College of Arts, Science and Technology. (2020). *MCAST artificial intelligence strategy: Roadmap 2025.* https://www.mcast.edu.mt/wp-content/uploads/AI-StrategyFinal.pdf.

4 OpenGov Asia. (2020). *Plans for cloud-first strategy and national AI framework revealed at 29th MSC Malaysia Implementation Council meeting.* https://opengovasia.com/plans-for-cloud-first-strategy-and-national-ai-framework-revealed-at-29th-msc-malaysia-implementation-council-meeting/

5 Ministry of the Economy and Innovation of the Republic of Lithuania. (2019). *Lithuanian artificial intelligence strategy.* https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_ENG(1).pdf

The strategies of the Group A countries are fundamental in nature and reflect both the general global problems of AI implementation and specific plans for reengineering various market and business sectors, digitalisation of many sectors of national economies and various spheres of social relations.

The main vector of AI technologies is aimed at the development and implementation of: systems with augmented and virtual reality and visualisation; broadband and other communication networks (5G, 6G); cloud computing; cyber-physical systems; security in cyberspace and Metaverse (biometric data); data mining, big data, database management; interaction technologies (motion recognition, speech technologies); Internet of Things; Internet services; location-based technologies (GPS, GIS); small and nanoelectronic smart systems; photonic, electronic and optical functional materials, robotics and autonomous systems, etc.

Let's consider the strategies of some countries in this group.

Saudi Arabia is a leader in the formation and development of AI technologies. The main governing body in this area is the Saudi Arabian Data and Artificial Intelligence Authority (SDAIA). SDAIA is a government agency that was created to organise work in the field of AI application and achieve the global goal of organising the implementation of the Data & AI program by 2030, providing training for 20 thousand AI developers, and creating an environment that will attract at least 300 startups in the field of artificial intelligence and data applications.

SDAIA has subordinate subsidiaries – the National Information Center (NIC), the National Data Management Office (NDMO) and the National Center for Artificial Intelligence (NCAI).

NIC is the national data bank that stores all government data, and which acts as the main state provider of analytical data processed using AI technologies. In turn, NIC is divided into:

The Estishraf Platform is an analytical unit that provides an opportunity for decision-makers and civil servants to study the materials, data and algorithms on the basis of which a decision proposal is submitted.

Absher is a platform that provides high-quality e-services to all citizens and allows them to use e-government services and transactions without having to visit government departments through four platforms Absher Individuals, Absher Business, Absher Recruitment and Absher Government.

Efaa is a national platform that aims to provide citizens, residents, visitors and business owners with the opportunity to know and review all their offences, and the corresponding actions taken by state institutions against them. The platform standardises, simplifies and streamlines procedures for detecting offences as it is linked to all relevant agencies dealing with offences. The goal of Efaa is to achieve discipline among members of society by encouraging citizens to comply with rules and laws.

National Data Bank is a nationwide data exchange platform that aims to collect and store relevant data sets from government agencies through real-time integration and processes to create a single source of reliable data.

Deem Cloud is a cloud computing platform that securely and reliably provides data to all government and non-government agencies.

The Unified National Platform GOV.SA is a national platform that serves more than 130 organisations for electronic identification of individuals for government and non-state providers of vital services. The platform includes mechanisms and standards of high security in accordance with the best global practices.

The National Data Management Office (NDMO) manages national data as a digital asset and is responsible for developing standards, policies, regulations, and compliance mechanisms, as well as developing regulatory frameworks, including areas such as data privacy and freedom of information.

The National Center for Artificial Intelligence (NCAI) manages the implementation of the AI strategy, organises research that focuses on innovations in data management and artificial intelligence, as well as the development of solutions in the field of artificial intelligence applications.

In addition, for the implementation of the Data & AI program, the Ministry of Communications and Information Technology and the Ministry of Education have introduced STEM (Science, Technology, Engineering and Mathematics) curricula, trainings and courses.

Thus, in order to promote research and innovation activities, the AI Center of Advanced Studies (Thakaa) aimed at the use of data and artificial intelligence was created.

At the same time, scientific research is being carried out to create a modern regulatory framework and the latest standards for the application of AI, data protection and privacy, which will include specifications on data collection, classification, data sharing, open data policy and freedom of information (Saudi Data and Artificial Intelligence Authority, 2020; Government of the United Arab Emirates, 2017)[1,2].

The Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 defines goals and measures for the development of artificial intelligence, the implementation of which should lead to economic growth, improvement of public services, development of scientific research and skills of personnel for work in the future. The implementation of the Strategy's measures should ensure the development and safe implementation of AI in accordance with internationally recognised ethical principles, as well as the achievement of the Sustainable Development Goals. According to a 2019 report, Serbia ranks 58th out of 194 countries.

The strategy for the development of artificial intelligence in the Republic of Serbia for the period 2020-2025 is in line with the European Artificial Intelligence Initiative, which defines the European Commission's policy on artificial intelligence. In this context, the Republic of Serbia, as a candidate for EU membership, as well as a member of the European Union Framework Programme for Research and Innovation, seeks to ensure the necessary level of compliance with the European Union, which will allow for full integration into the European Research Area and more fruitful cooperation.

This Strategy is considered to be the most detailed action plan among European countries, which was created together with the simultaneous modernisation of a number

1 Saudi Data and Artificial Intelligence Authority. (2020). *National strategy for data & AI: Strategy narrative—Realizing our best tomorrow.* https://ai.sa/Brochure_NSDAI_Summit%20version_EN.pdf).

2 Government of the United Arab Emirates. (2017). *UAE national strategy for artificial intelligence 2031.* https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.p

of national laws, such as: the Law "On Personal Data Protection", the Law "On the Basics of the Education System", the Law "On Science and Research", the Law "On Innovative Activity", the Law "On the Science Foundation of the Republic of Serbia", the Law "On Information Security", "Strategy for Scientific and Technological Development of the Republic of Serbia for the period 2016-2020", "Proposals of the Program for the Development of E-Governance in the Republic of Serbia for the period from 2019 to 2022 and an action plan for its implementation", "Strategy for the Development of the Information Society in the Republic of Serbia until 2020", "Strategy for the Development of Information Security for the Period 2017-2020", "Strategy for the Development of the Information Technology Industry for the Period 2017-2020", "Strategy for the Development of New Generation Networks until 2023", etc.

The national priorities of the Republic of Serbia are defined:

- modernisation of the education system, development of competencies for the future needs of the labour market and professions directly related to AI and other professions that change under the influence of AI;
- adaptation of the business sector to new working models and the development of new business entities whose business is based on the use of AI;
- development of research activities and the emergence of highly competitive experts in the field of AI application and its implementation;
- legal regulation in all areas is adapted to the new circumstances caused by the use of AI, the requirements of new business models and the development of products and services based on AI, taking into account protection from potential negative consequences;
- comprehensive study of the understanding of the ethical aspects of the use of AI, taking into account the principles of preserving individual freedom, justice and equality, avoiding harm, openness, transparency and sustainability (Government of the Republic of Serbia, 2019)[1].

The AI development strategy of the People's Republic of China is based on the real achievements of domestic scientists and researchers in the field of information and communication technologies. China has made significant strides in the field of AI in terms of the number of international published scientific and technical papers and the number of patented inventions. It also leads in the development of voice recognition, visual face recognition and biometric identification technologies. Despite these achievements, China states that its scientists, research institutions and enterprises do not yet have sufficient international influence on AI technology cycles and technologies due to the lack of a systematic research and development plan, and the implemented achievements in the field of artificial intelligence are currently not in significant external demand. The global objective of China's AI strategy is to comprehensively enhance society's productive forces, national power, and national competitiveness, in order to provide strong support and accelerate the construction of a new type of innovation nation, global science and technological power, and the rejuvenation of the Chinese nation. China's strategy outlines such areas of development of AI technologies as: creating a digital economy; building a

1 Government of the Republic of Serbia. (2019). *Strategy for the development of artificial intelligence in the Republic of Serbia for the period 2020–2025.* https://www.srbija.gov.rs/extfile/en/420876/strategy_artificial_intelligence_2020-2025_en.pd

smart society; protection of national security; building knowledge clusters, technology clusters and industrial clusters interintegrated with talented citizens and cultural representatives to comprehensively support the ecosystem. The strategy envisions that the AI industry established during the first phase will be widely used in intelligent manufacturing, smart medicine, smart eco-cities, smart agriculture, national defence construction and other industries, with the investment scale of the main AI industry being more than 400 billion yuan, and the investment scale of related industries exceeding 5 trillion yuan. By 2025, China has established initial laws and regulations on artificial intelligence, ethical norms and policy systems, as well as the formation of an assessment of the security of AI and the possibility of its control. By 2030, Chinese scientific and theoretical research on AI, AI technologies and applications should reach the world level, making China intend to become the world's main AI innovation centre, the most innovative country in the world according to the ranking of innovations in the state's economy. China also plans to form a more modern theory and technology of next-generation AI. The country can achieve great breakthroughs in creating ASI development.

Therefore, through the introduction of innovative AI technologies of a higher level, a high level of competitiveness of the AI industry will be achieved. of the main AI industry, exceeding 1 trillion yuan, and with a scale of related industries exceeding 10 trillion yuan. China will establish a number of the world's leading AI innovation technologies, training centres, implement comprehensive laws and regulations on artificial intelligence, and ethical norms and policies (China.org.cn, 2019; State Council of the People's Republic of China, 2017)[1, 2].

The super objective of the United States of America's AI Development Strategy, announced by the 45th and 46th Presidents of the United States, is to promote the creation of an international environment that supports American AI innovation, and foreign nations should internationally promote the development of a global environment that supports American AI, research and innovation, and open markets for American artificial intelligence industries. The United States should also work with its international partners in the G7 and G20 to adopt similar principles for the development of artificial intelligence. The United States also intends to reduce barriers to the development, testing, deployment, and deployment of AI technologies by providing guidance for AI governance in line with the values of the American nation and driving the development of appropriate AI technical standards. The American strategy is characterised by the fact that it has certain unique positions. Thus, AI technologies are supposed to be used to improve the provision and efficiency of public services to the American people and ensure privacy, civil rights, and civil liberties. It is planned to create an AI Center of Excellence in order to determine by federal agencies the best practices for implementing AI in their organisations (Office of Management and Budget, 2013)[3].

Attention should be paid to the declaration that the federal government cannot and should not be the main driver of the United States' AI innovation. At the same time, it is

1 China.org.cn. (2019, February 22). *National new-generation AI innovation & development pilot zone established in Beijing.* http://www.china.org.cn/china/2019-02/22/content_74493744.htm

2 State Council of the People's Republic of China. (2017). *Notice on the issuance of the next generation artificial intelligence development plan.* https://na-production.s3.amazonaws.com/documents/translation-fulltext-8.1.17.pdf

3 Office of Management and Budget, Executive Office of the President. (2013). *Open data policy: Managing information as an asset (M-13-13).* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2013/m-13-13.pdf

noted that the creation and maintenance of a large-scale national AI research and development ecosystem requires federal investment and policies to promote strong cooperation between academia, industry and the federal government. It is the government that has a crucial role in providing targeted funding for research and development, supporting long-term basic research that stimulates future technological breakthroughs, and directing investments in AI research and development. That is, federal resources will still be directed to accelerate national research and development in the field of AI.

The plan identifies key areas to focus on: developing effective methods for human-AI collaboration; understanding and biasing the ethical, legal, and social implications of AI applications; ensuring human safety and security of AI systems; developing shared publicly available datasets and environments for AI training and testing; measuring and evaluating AI technologies through standards and benchmarks; better understanding the research and development needs of the national workforce in the field of artificial intelligence; expanding public-private partnerships to accelerate the development of AI. The United States has singled out a number of federal agencies that are entrusted with certain government tasks for the development of AI technologies. The National Science Foundation, which supports transformational basic research in AI with investments. The Defense Advanced Research Projects Agency, which is currently a leader in AI research and invests in the "third wave" of AI systems that have characteristics important for military and critical security systems, namely the ability to work with contextual data and explanations of actions and outcomes. The U.S. Department of Defense's Joint Center for Artificial Intelligence conducts research on scaling AI and drives the acceleration of AI research in the military field. The National Institute of Standards and Technology (NIST) is a major leader in basic research that informs the development of technical standards for all varieties of AI. The Department of Energy is leading the development of a high-performance computing infrastructure that supports AI research. The Department of Veterans Affairs, in partnership with the Department of Energy, conducts research and secure analysis of big digital health and genomic data to help improve veterans' health care and in areas such as suicide, cancer, and heart disease prevention. The National Institutes of Health is researching effective ways AI can be used in medicine, such as diagnosing diseases or personalising treatment. The Department of Transportation is introducing the development of documentation for the safe integration of automated vehicles using AI techniques on the roads. The Department of Labor, Commerce and Human Health of the Ministry of Health is studying the impact of automated systems with AI on the workforce, as well as what new skills and competencies will be needed by the workforce due to the digitalisation of the economy. The National Oceanic and Atmospheric Administration uses AI to process satellite weather data to predict hurricanes and natural phenomena. The Interagency Working Group on AI Research and Development, which is comprised of program managers and technical experts from across the federal government and helps coordinate interagency programs, R&D and AI efforts, and simultaneously serves as an interagency AI research centre (Office of

Management and Budget, 2020; (National Institute of Standards and Technology, 2019; Carnahan & Phelps, 2018; Carnahan & Phelps, 2018)[1, 2, 3, 4].

A general analysis of AI development strategies in different countries indicates that society and governments understand the importance of using modern information and communication technologies, including AI technologies. The development of digital technologies is an integral aspect of the development of society and often contributes to the acceleration of its positive development. At the same time, humanity is quite realistically aware of the risks of uncontrolled use of AI and understands the need to apply legal regulation of its use through standards and regulations. AI development strategies are at the same time indicators of the state of general digitalisation of a particular state and the readiness to redirect resources to the scope of AI application.

It is advisable for Ukraine to carefully study these documents and the results achieved by the country at different stages of implementation. The analysis of strategies can become the basis for the formation of a national strategy for the development of AI in Ukraine. It should also be noted that so far the strategies have very carefully noted the problems of legal regulation of the use of AI technologies. At the current stage, legal regulation is proposed to be carried out through the development and application of standards in the field of AI and voluntary certification of AI products. The problem of a comprehensive legislative approach to the legal regulation of AI is in a discussion format. This is inherent in all countries of the world.

2.1.8. Problems of morality of autonomous artificial intelligence.

Another aspect that has been concentrated in the problem of the morality of autonomous artificial intelligence and has been of concern to scientists and researchers since they began to apply fast mathematical algorithms for processing large amounts of data. In 1956, at a scientific conference at Dartmouth College (USA), the concept of "artificial intelligence" was born with the light hand of the researchers present. Today, these are ultra-modern, extremely complex and high-speed algorithms that work with big data to form initial predictions with a given probabilities that are used for decision-making in various fields of science, technology and the social sphere. The problems of artificial intelligence and the Metaverse are covered in the previous work, which forms the key postulates of the development of social relations using Metaverse technologies, artificial intelligence, artificial neural networks, robotic systems (Kostenko, 2022d)[5]. Let's consider the problems of the development of autonomous AI.

---

1 Office of Management and Budget, Executive Office of the President. (2020). *Guidance for regulation of artificial intelligence applications (M-21-06).* https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf).

2 National Institute of Standards and Technology, U.S. Department of Commerce. (2019, August 9). *U.S. leadership in AI: A plan for federal engagement in developing technical standards and related tools.* https://www.nist.gov/topics/artificial-intelligence/plan-federal-engagement-developing-ai-technical-standards-and-related

3 Carnahan, L., & Phelps, A. (2018, September). *ABC's of conformity assessment* (NIST Special Publication 2000-01). National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.2000-01

4 Carnahan, L., & Phelps, A. (2018, September). *Conformity assessment considerations for federal agencies* (NIST Special Publication 2000-02). National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.2000-02

5 Kostenko, O. V. (2022d). Electronic jurisdiction, metaverse, artificial intelligence, digital personality, digital avatar, neural networks: Theory, practice, perspective. *World Science, 1*(73). https://doi.org/10.31435/rsglobal_ws/30012022/7751.

Today, there are numerous scientific discussions around the use of AI. One of the key discussions is the morality of autonomous AI.

At the same time, there are two hypotheses among scientists that relate to the morality of autonomous AI. According to the first hypothesis, autonomous AI can be exclusively moral from a philosophical point of view and exist alongside humanity, while fulfilling the tasks of positive sustainable development of society. According to the second hypothesis, the possibility of forming an autonomous AI (artificially or spontaneously) that will begin to act independently, that is, without receiving instructions from a person, and obsessed with the goal of dominating or destroying the human race, is not excluded.

It is quite obvious that scientists have focused on the research and development of positively moral AI. Currently, the models of moral AI are diverse: mixed, capable of applying different algorithms and methods of data processing; endowed with the functions of "making" moral decisions (Wallach & Allen, 2005)[1]; based on the OSI model, which consistently "top-down" fulfils a set of ethical rules (Osvita-Plaza, n.d.)[2]; on anti-OSI with the implementation of certain ethical rules "from the bottom up" (Anderson & Anderson, 2008)[3]; reinforcement learning systems, i.e. not only data processing, but also with additional testing or the choice of different strategies to achieve maximum results, etc. (Figure 26).

It is also worth noting that the main efforts of scientists are aimed at the technical and legal limitation of AI. Thus, the expert Mady Delvaux in Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL)) (Delvaux, 2017)[4] emphasised that the technological achievements of robotics stimulate the introduction by robots of some autonomous and cognitive functions inherent only in humans, such as: the ability to learn from experience, make independent decisions. However, this can encourage robots to take destructive actions that have harmful consequences and for which, by analogy with humans, legal responsibility should occur. At the same time, manufacturers, owners, software developers, users, military commanders, etc., are still responsible for the actions of non-autonomous or partially autonomous robots (Figure 26). Until now, the only legal act that defines liability for damage caused by work is Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States on liability for defective products (European Parliamentary Research Service, 2016)[5].

1 Wallach, W., & Allen, C. (2005). Android ethics: Bottom-up and top-down approaches for modeling human moral faculties. https://www.semanticscholar.org/paper/Android-Ethics-%3A-Bottom-up-and-Top-down-Approaches-Wallach-Allen/a65e0e2c951c447f827107786c4b6deeb2b71226

2 Osvita-Plaza. (n.d.). Etalonna model vzaiemodii vidkrytykh system (EMVVS, OSI – Open System Interconnect). Rivnevi protokoly [Reference model of open systems interaction (OSI). Layered protocols]. http://osvita-plaza.in.ua/publ/45-1-0-435

3 Anderson, M., & Anderson, S. L. (2008). ETHEL: Toward a principled ethical eldercare robot. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.177.5971.

4 Delvaux, M. (2017). *Report with recommendations to the Commission on civil law rules on robotics.* European Parliament. https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.htm

5 European Parliamentary Research Service. (2016). *Cost of non-Europe in robotics and artificial intelligence.* European Parliament. http://www.europarl.europa.eu/committees/en/juri/robotics.html?Tab=Introductio

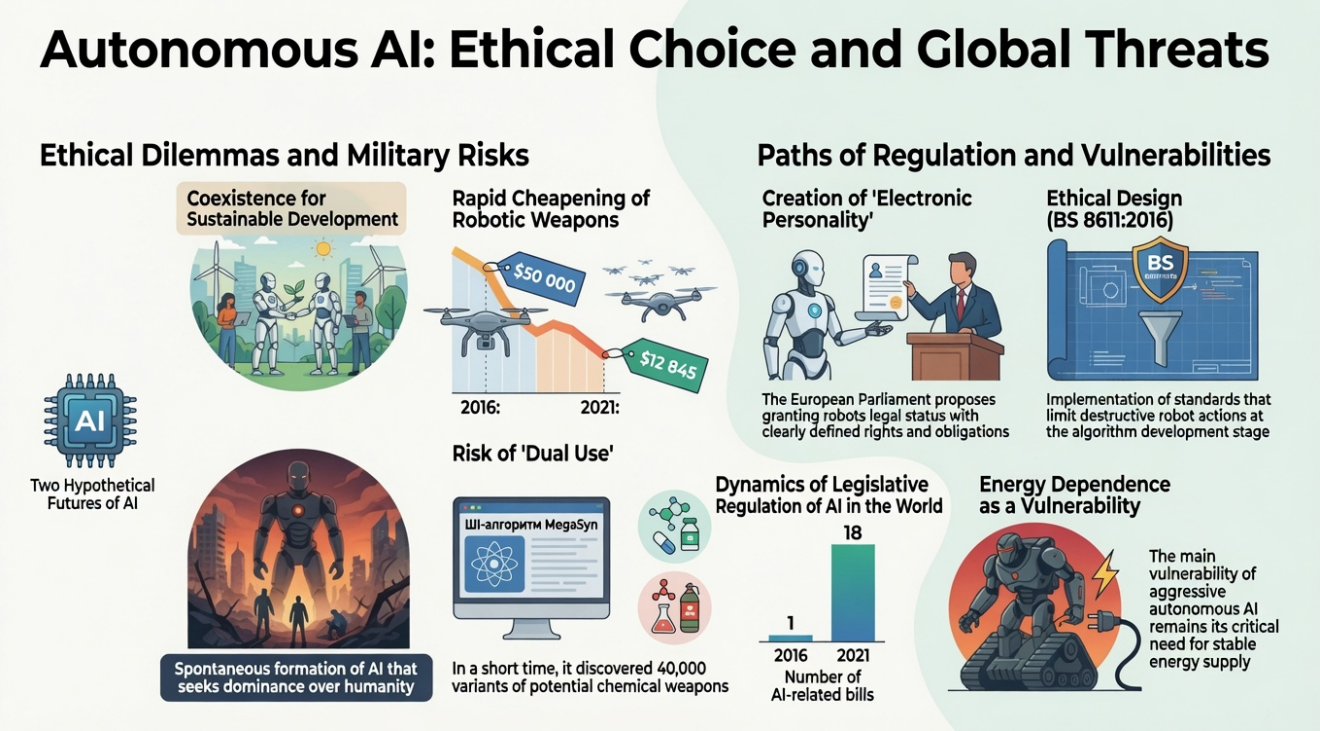


Figure 26. Autonomous AI: challenges and threats

The European Parliamentary Research Service (EPRS) and the European Parliament's Legal Affairs Committee are developing recommendations to improve the civil and ethical aspects of robotics, which propose to establish a register of robots and an appropriate EU Agency for Robotics, as well as to establish civil liability for damages caused by robots in accordance with and in proportion to the actual level of instructions provided according to the degree of its autonomy. Planned implementation of technical, ethical and regulatory expertise in the field of robotics and the development of the "Code of Ethical Conduct for Robotics Engineers" and the "Code of Research Ethics Committees" (European Parliamentary Research Service, 2017)[1].

In September 2016, the British Standards Institution issued the BS 8611:2016 standard "Robots and robotic devices. Guidelines for the Ethical Design and Application of Robots and Robotic Systems" (British Standards Institution, 2016[2]). Thus, in 2019, the Expert Group on Responsibility and New Technologies – Emerging Technologies, which was established by the European Commission, in the Report "Responsibility for Artificial Intelligence and Other Digital Technologies" indicated that the regimes of responsibility for the implementation of AI and IoT should provide sufficient safeguards to minimise the risks of harm that these technologies may cause (Expert Group on Liability and New Technologies – New Technologies Formation, 2019)[3].

1 European Parliamentary Research Service. (2017). *Civil law rules on robotics.* European Parliament. http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599250/EPRS_ATA(2017)599250_EN.pd

2 British Standards Institution. (2016). *BS 8611:2016 robots and robotic devices: Guide to the ethical design and application of robots and robotic systems.* https://www.en-standard.eu/bs-8611-2016-robots-and-robotic-devices-guide-to-the-ethical-design-and-application-of-robots-and-robotic-systems/

3 Expert Group on Liability and New Technologies – New Technologies Formation. (2019). *Report from the Expert Group on Liability and New Technologies: Liability for artificial intelligence and other emerging digital technologies*. Publications Office of the European Union. https://doi.org/10.2838/25362.

In addition, in 2016, the Executive office of the President National Science and Technology Council, Washington, D.C. 20502, the Technology Committee prepared a review "Preparing for the Future of Artificial Intelligence" on the prospects for the use of AI, since it is considered unacceptable to use certain AI predictions regarding the development of humanity and at the same time to neglect the decisions made by people on the same issues. In addition, it is necessary to regulate the use of artificial intelligence to control the equipment of the physical world, especially if it is directly related to the safety of people (Executive Office of the President, National Science and Technology Council, 2016)[1].

In 2017, the European Parliament published its set of general recommendations on how to implement ethics in robots, as well as proposals to define their legal status as an "electronic person with special rights and obligations". Google presented "Perspectives on Issues in AI Governance", which highlights the general problems of using artificial intelligence at the conceptual level (Google, n.d.)[2].

At the beginning of 2022, Stanford University published the annual study "Artificial Intelligence Index Report 2022", which contains the results of a survey of robotics researchers from around the world, data on global legislation on artificial intelligence in 25 countries, as well as a section with an in-depth analysis of technical indicators of AI ethics provided by academic, private and non-profit organisations.

An analysis of legislative activity in 25 countries shows that the number of draft laws containing AI and the number of laws adopted increased from 1 in 2016 to 18 in 2021. It was Spain, the United Kingdom and the United States that passed the largest number of bills related to artificial intelligence.

In our opinion, the fact noted in the Index Report that robotic weapons are becoming cheaper and available for mass use is alarming, namely: the average price of robotic weapons over the past six years has quadrupled from $50,000 per unit in 2016 to $12,845 in 2021[3].

That is, technological improvements can provide greater precision in the use of weapons and greater "humanity" of military operations. It is high-precision ammunition that allows you to end the war with fewer weapons spent and collateral damage, and remotely piloted vehicles can reduce risks for military personnel.

At the same time, it should be noted that scientists do not know for sure what AI algorithms are currently being developed and used in the military sphere. It is considered very risky to move away from direct human control over guided and autonomous weapon systems.

Also in November 2012, the U.S. Department of Defense Directive No. 3000.09 "Autonomy in Weapon Systems" came into force, which establishes Department of Defense policy and legal responsibility for the development and use of autonomous and

1 Executive Office of the President, National Science and Technology Council. (2016, October 12). *Preparing for the future of artificial intelligence*. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

2 Google. (n.d.). *Perspectives on issues in AI governance*. https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf.

3 Stanford Institute for Human-Centered Artificial Intelligence. (2022). *Artificial intelligence index report 2022*. https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf

semi-autonomous functions in weapons systems, including manned and unmanned platforms, and establishes guidelines designed to minimise the likelihood and consequences of failure in autonomous and semi-autonomous weapons systems, which can lead to unintentional losses[1].

According to some publications and informational reports, we can state that the use of AI is currently at the stage of implementation in certain types of autonomous weapons. For example, Heron Systems successfully conducted virtual air battles between artificial intelligence and the pilot of an F-16 fighter of the US Air Force at the electronic test site of the US Department of Defense Advanced Research Projects (DARPA)[2].

In addition, scientists from the private pharmaceutical company Collaborations Pharmaceuticals recently changed several commands in the artificial intelligence algorithm for research purposes in order to speed up the MegaSyn molecule generator to filter out toxic substances during the search for new drugs. Instead, the MegaSyn molecule generator specifically identified 40 thousand variants of potential biological and chemical weapons based on known combat poisons – including the "Newcomer". Many new toxic molecules have also been developed that are potentially even more dangerous than those already known (24 Kanal Tech, n.d.)[3].

Moral AI and requirements for its ethical application can become declarative and unrealistic in the case of the use of AI technologies by dictatorial regimes. As evidenced by the facts during the modern war unleashed by russia against democratic Ukraine, the vast majority of conventions, international regulations, ethical norms can be brutally neglected. Therefore, international organisations become powerless against brazen violations of the world order and decades. In fact, Russia today acquires the status of an aggressive invader, which is guided only by its own ideas about the world order. In such a situation, the use of AI in the military sphere may not only be uncontrolled, but also involve the fulfilment of tasks to destroy people. Russia's aggression against Ukraine raises many questions about the future structure of society. It is in countries with dictatorial regimes that one of these issues arises: the possibility of the emergence and existence of autonomous aggressive AI. Let's imagine the possibility of the emergence of autonomous aggressive AI in the near future, taking into account the development of digital humanity in the Metaverse.

We propose to consider the hypothesis according to which aggressive autonomous AI can exist with a certain degree of probability. So, in our opinion, it is unlikely that it will have the appearance of a supercomputer that is created and functions in a certain place. The most rationally autonomous AI will look like a group of independent computing clusters, like botnets distributed in space, which are configured to perform specific tasks-algorithms. Cluster groups may be grouped according to the OSI model, in

1 U.S. Department of Defense. (2012). *Directive No. 3000.09: Autonomy in weapon systems*. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

2 V Mynysterstve oborony SShA provely virtualnyi boi yskusstvennoho intellekta s pilotom ystrebitelia F-16. Alhorytm ispytival maksimalnye vozmozhnosti cheloveka i samoleta [The U.S. Department of Defense conducted a virtual battle between artificial intelligence and an F-16 fighter pilot. The algorithm tested the maximum capabilities of the human and the aircraft]. (n.d.). *NV Techno*. https://techno.nv.ua/innovations/algoritm-pobedil-pilota-vvs-v-boyu-50108456.html

3 Shtuchnyi intelekt dlia poshuku likiv vyhadav 40 tysiach variantiv khimichnoi zbroi [Artificial intelligence for drug discovery generated 40 thousand variants of chemical weapons]. (n.d.). *24 Kanal Tech*. https://tech.24tv.ua/shtuchniy-intelekt-dlya-poshuku-likiv-vigadav-40-tisyach-variantiv_n1915202

which each layer is characterised by its own set of AI clusters. Several clusters will definitely be formed for strategic decision-making, as well as for the application of mechanical and biotechnical android robots. This is the most efficient and least vulnerable configuration to external factors.

What is the goal and what tasks will the autonomous aggressive AI pursue? It is believed that autonomous AI will use data from the historical development of humanity to form the goal and measures to achieve it, since there is no other data on the development of civilisation, for example, extraterrestrial. Unfortunately, the history of mankind, and especially in recent years, is full of negative examples of hostility and aggression for people. Numerous military simulators, military AI, electronic means of analytical assessment of past and current military conflicts actually create a modern library on the basis of which aggressive autonomous AI can independently formulate strategies and tactics for conducting destructive actions against humanity.

Thus, to choose a strategy for attacking humanity, autonomous AI has a fairly wide base of both historical examples of military operations and current war. Therefore, the strategy, tactics and methods of waging war against humanity are not a big secret. There are a lot of wars and military conflicts in the history of mankind. There are quite a few reasons for which they arose, but in general they converge to three: a) seizure of territory; b) seizure of resources; c) seizure of labour and reproductive power. It is possible to assume that for aggressive autonomous AI, these grounds will also be basic. Points "a" and "b" are likely to be combined in the capture of large cities and megacities, since it is here that huge resources are concentrated in a small area: ferrous and non-ferrous metals, data transmission infrastructure, computers, electronic gadgets, data centres, servers, IoT devices and many other things necessary to provide various clusters, including mechanical and biotechnical android robots. Therefore, autonomous AI does not need to physically extract minerals from the bowels of the earth and create a full production cycle. Autonomous AI does not need to create an army of robots of 5 billion units. Effective autonomous robotic weapons controlled by AI are capable of being many times more effective than any army with the compact forces necessary to keep the ecosystem for robots in good condition. However, the autonomous AI model has one vulnerable drawback – the provision of energy. The destruction of AI energy supply infrastructure is the destruction of AI clusters or autonomous AI itself. We will leave point "c" without consideration, since the author believes that humanity in the near future will take decisive steps to control the development and use of all varieties and forms of AI, which will make it impossible to use it to the detriment of humanity. Is it possible that an aggressive autonomous AI will attack humanity? Yes, in general, such a scenario must be considered at least in order to prevent it and avoid it in time.

It is advisable to create a unified international system for recording and responding to incidents in systems with artificial intelligence algorithms, starting with the formation of an international Standard Model of Technical, Biological, Financial, Economic, Political and Military Threats from the Use of (Authorized and Unauthorized) AI-Based Systems (Kostenko & Furashev, 2022e)[1].

1 Kostenko, O. V., &Furashev, V. M. (2022e). *Praktychni pytannia pravovoho rehuliuvannia zastosuvannia tekhnolohii zi shtuchnym intelektom* [Practical issues of legal regulation of the application of artificial intelligence technologies]. In

At the same time, it is also necessary to intensify the work of international organisations on the development and creation of the Model Law "On Artificial Intelligence", which will form the basis of relevant national legislative acts. In turn, scientists need to form a single categorical and conceptual apparatus in the field of AI as soon as possible and ensure its maximum distribution for simultaneous application in the legislative jurisdictions of different states.

2.2. Internet of Things in the Metaverse Structure: Legal Aspects of Integration of Physical and Virtual Environments

2.2.1. Internet of Things

The growing interest in the formation of high-level immersive and intellectualised digital environments capable of ensuring continuous human interaction with next-generation cyber-physical systems naturally brings to the fore a set of legal problems covering the subject of information law, administrative and legal regulation and related fields. Such environments, which cover the continuum from the extended physical to the fully virtualised space, in the future it is advisable to name the Metaverse as a special information and technological ecosystem within which the production, circulation and legal significance of data take place, the implementation of digital rights, as well as the formation of specific regimes of identification, access and responsibility.

Historically, Industrial Automation and Control Systems (IACS) have evolved as relatively isolated technological circuits, detached from corporate ICT networks for reasons of reliability, production continuity and cybersecurity. Where there was a need to interact with the "office" digital infrastructure, a zoned architecture dominated with the use of firewalls and/or demilitarised zones (DMZs), which served as a technical barrier and at the same time, a tool for providing controlled access to critical control components. In the legal dimension, such isolation actually reduced the risks of uncontrolled data flow, third-party interference, and complex liability issues, since the boundaries of the system, its "perimeter of trust" and the circle of responsible persons were relatively defined (Baranov, 2019)[1].

International scientific innovations in human life: Proceedings of the 9th International scientific and practical conference 255–260. Cognum Publishing House. https://doi.org/10.13140/RG.2.2.12744.39682

1 Baranov, O. A. (2019). Internet of Things and Law: A Look into the Future of the Internet of Things: Problems of Legal Regulation and Implementation. *Collection of Materials Supplementary Participant, III Scientific and Practical Conf*. 7–13. https://ippi.org.ua/sites/default/files/maket_ot_20.11.19._1.pdf

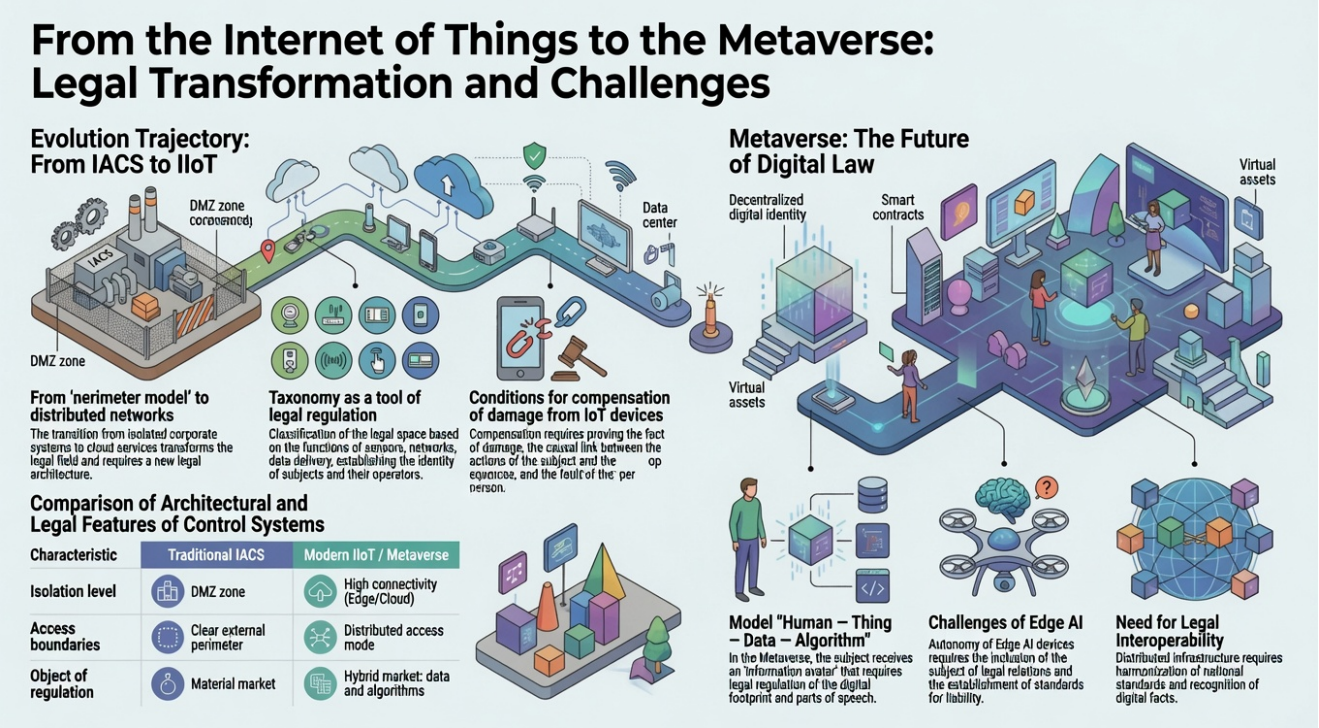


Figure 27. Metaverse: IoT

Instead, the mass adoption and deployment of IoT technologies is causing structural (architectural) changes in IACS, primarily by significantly increasing the level of connectivity of industrial circuits to general-purpose networks and cloud/edge services. This means moving from a perimeter protection model to more complex, distributed access control, logging, and security modes, where not only the physical boundaries of the object, but also access policies, event logs, remote administration settings, and algorithmic process control decisions become legally significant. In view of the above, IIoT appears as a factor that transforms not only the technical risk profile, but also the legal architecture of liability in the field of industrial safety, labour protection, information security and data protection (Figure 27).

The analysis of relevant partial IoT taxonomies identifies features suitable for systematising the industrial IoT segment. This is of applied importance for law enforcement, since taxonomy allows:

1) classify IIoT devices and components by functional role (sensors, actuators, gateways, controllers, analytical nodes);

2) to determine the points of data collection/processing and, as a result, the legal regime of these data (industrial data, trade secrets, personal data of employees, telemetry);

3) establish chains of responsibility between the manufacturer, integrator, operator, service provider and end user. Thus, classification is the basis for legal regulation, since it allows you to tie legal obligations to specific technical roles and processes.

In the legal plane, such a structure can be interpreted as a tool for evidence-based governance and compliance: it helps to document the system (asset inventory), determine the criticality of components, model risks and install appropriate safeguards. It is important that the relationship between architecture → risk → the standard of due diligence → responsibility is fundamental for law here, because it is through a properly described architecture that it is possible to justify whether reasonable security measures

have been taken, whether there was foreseeability of the incident and whether there was a causal relationship between organisational deficiencies and damage (Sisinni et al., 2018)[1].

It should be noted that the problem of systematisation of norms in the field of IoT is an urgent problem (Kharytonov & Kharytonova, 2017)[2]. This can be investigated on the example of the variable development of the concept of IoT, which is constantly being improved and developing and today the following variants of the definition of "Internet of Things (IoT)" are actively used:

> devices, vehicles, structures and other objects - embedded in electronics, software, sensors and network connectivity that allows these objects to collect and exchange data (International Telecommunication Union, n.d.)[3];
>
> a set of interacting technical systems and complexes consisting of microprocessors, sensors, devices, data transmission systems, local and/or distributed computing resources and software, including artificial intelligence programs, based on the use of a huge amount of data and the Internet and intended for the implementation of social relations, in particular, related to the provision of services or work with the direct participation or without the participation of the subjects of these relations (legal entities or individuals) (Baranov, 2018)[4];
>
> a global infrastructure for the information society that provides advanced services through the interconnection of (physical and virtual) things based on existing and developed interacting information and communication technologies (International Telecommunication Union, 2012)[5];
>
> a worldwide network of interconnected objects uniquely addressed based on standard communication protocols (Kong et al., n.d.)[6];
>
> IoT is a paradigm by which existing networked devices are connected to real-world objects such as home appliances, vehicles, and healthcare (Yan et al., 2008) (Yan et al., 2008)[7];
>
> a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols, where physical and virtual "things" have identities, physical attributes and virtual identities and their

1 Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics, 14*(11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491

2 Kharitonov, E. O., & Kharitonova, O. I. (2017). Category "Internet of Things" and civil legal relations. *Scientific Works of the National University "Odessa Law Academy", 20,* 169–177. https://hdl.handle.net/11300/12514

3 International Telecommunication Union. (n.d.). *Internet of Things Global Standards Initiative*. https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

4 Baranov O.A. (2019). Internet of Things (IoT) and blockchain. *Information and Law. 5*(4). 59-71. https://doi.org/10.37750/2616-6798.2018.1(24).270747.

5 International Telecommunication Union (ITU). ITU-T Recommendation ITU-T Y.2060 (06/2012). International Telecommunication Union. (2012). *Overview of the Internet of things* (Recommendation ITU-T Y.2060). https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

6 Kong, N., Jungsoo, P., Crespi, N., Lee, G., & Chong, I. (n.d.). *The Internet of Things: Concept and problem statement*. https://www.semanticscholar.org/paper/The-Internet-of-Things-Concept-and-Problem-Kong-Jungsoo/5ef74cba1f2836fa895aa9f336bc88e8246e711d

7 Yan, L., Zhang, Y., Yang, L. T., & Ning, H. (2008). *The Internet of Things: From RFID to the next-generation pervasive networked*. CRC Press. https://doi.org/10.1201/9781420052824

uses, intelligent interfaces are seamlessly integrated into the information network (International Telecommunication Union, 2005)[1].

The development of national legislation in modern information areas is not always advisable to carry out through the direct intervention of English-language terms. Based on the results of the analysis of foreign literature, it can be concluded that many years of experience of European terminologists prove that it is not always necessary to introduce foreign words into circulation in the presence of generally accepted national ones (Bieliakov et al., 2013; Kostenko, 2021d)[2, 3].

The main problems of the Internet of Things include information security and personal data protection (Baranov & Bryzhko, 2016; Pylypchuk et al., 2017)[4, 5]: identification of mechanisms for the implementation of the principle of prior consent to the use and destruction of personal data; legal impact on the regulation of cross-border flows of personal data; use of personal data by intellectual complexes that operate without the participation of subjects (legal entities or individuals) (Katkova, 2020; Kharytonov & Kharytonova, 2018)[6, 7].

The problem of protecting human rights and compensation for damage caused by the Internet of Things arises already in the case when the fact of an offence has occurred. In this case, it should be noted that the conditions for compensation for damage caused by a device included in the Internet of Things will include:

1) the presence of damage;

2) illegality of the behaviour of the person causing damage (which will be the manufacturer of the device), which is expressed in the failure to take measures to ensure the safety of the device;

3) causal relationship between the behaviour of the instigator and the damage;

4) the guilt of the person causing the damage (Nekit, 2017)[8].

In view of the above, it is methodologically correct to derive the problems of the Metaverse from the evolution of the Internet of Things, since it was IoT that formed the basic model of integration of physical and digital environments and thus a new type of legal relationship "person – thing – data – algorithm". Within this model, the key is to provide objects with the ability to contextually "understand" the environment (through sensors, telemetry, logging) and expand the possibilities of perception and control by users — from consumer automation to complex industrial systems. In the legal

1 International Telecommunication Union. (2005). *The Internet of Things*. https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

2 Belyakov K. I., Lande D. V., Novikova V. G. (2013) Information Legislation of Ukraine: Short Stories of 2013. *Legal Bulletin of Ukraine. 52* (965) 14-15.

3 Kostenko, O.V. (2021d) Identity Data Management (Identification): Problems of Conceptual and Categorical Apparatus: n *The latest development of the modern legal sciences and education in Ukraine and EU countries: An experience, challenges, expectations*. 317–330.

4 Baranov, O. A., & Bryzhko, V. M. (2016). Personal Data Protection in the Internet of Things. *Information and Law*, 2, 85–91.

5 Pylypchuk, V. G., Bryzhko, V. M., Baranov, O. A., & Melnyk, K. S. (2017). *Formation and development of the legal basis and system of personal data protection in Ukraine.*

6 Katkova, T. G. (2020). Artificial Intelligence in Ukraine: Legal Aspects. *Law and Society*, 6, 46–55.

7 Kharitonov E. O., & Kharitonova O. I. (2018). To the problem of civil legal personality of robots. In *the Internet of Things: problems of legal regulation and implementation: materials of the II scientific and practical conf.*168.

8 Nekit, K. H. (2017). Problemy zabezpechennia informatsiinoi bezpeky ta vidshkoduvannia shkody, zapodiianoi prystroiamy, pidkliuchenymy do internetu rechei [Problems of ensuring information security and compensation for damage caused by devices connected to the internet of things]. *Chasopys tsyvilistyky*, *27*, 107–111.

dimension, this means that the classical object of law (thing) acquires an information layer, and therefore, the legal regime should cover not only the material component, but also data, software, algorithmic control rules and interaction protocols.

Further intellectualisation of IoT, accompanied by the spread of edge artificial intelligence, significantly complicates the legal qualification of system behaviour and the distribution of legal responsibility. Edge AI collects and processes data, as well as decision-making at the device or local node level, reducing the role of centralised control and increasing autonomy. This, in turn, exacerbates the problems of determining the subject of responsibility (manufacturer, operator, platform provider, integrator, user), due diligence limits and security standards, as well as issues of evidence and traceability of system actions (logging, audit traces, "storage chain" of digital evidence).

In the Metaverse environment, these challenges receive an additional dimension, since interaction with cyber-physical objects and their digital twins takes place in a virtualised space, where data becomes not just a technical resource, but a legally relevant factor that can generate, change or terminate rights and obligations. In this area, special attention is required:

1) legal regime of data (personal, industrial, telemetry) and their classification;

2) digital identity and authentication modes, including identity management;

3) conditions for lawful processing, minimisation, anonymisation/pseudonymisation and ensuring information security;

4) legal qualification of algorithmic decisions and requirements for algorithmic transparency and accountability.

Moving on to the next aspect, it is worth noting that the integration of IoT and immersive platforms in the Metaverse environment gives rise to complex conflict-of-laws issues regarding jurisdiction, applicable law, and enforcement of decisions, since the infrastructure can be distributed among different states, and users can be in multiple legal orders. This creates an objective need for legal interoperability: harmonisation of minimum standards of evidence, procedural safeguards, cybersecurity requirements, and mechanisms for the mutual recognition of digital facts and identification attributes, without which the provision of rights and freedoms in the Metaverse will remain fragmented.

Based on the analysis, it can be concluded that the Metaverse should be considered as a new level of development of the information society, within which the Internet of Things is transformed from an infrastructure technology into a system-forming element of digital reality. Such a transformation objectively requires a revision of the established legal models "subject – object – legal relationship" and the formation of new approaches to the legal regulation of human interaction, algorithms and cyber-physical objects. The trajectory of "IoT - Intelligent IoT - Metaverse" is not only technological, but also normative: it requires a revision of the classic legal models "subject - object - legal relationship" and the formation of a legal ontology capable of describing mixed (hybrid) relationships in cyber-physical and virtual environments. In such an ontology, data and algorithmic processes should be considered as elements of the legal regime along with tangible things, and digital procedures should be considered as tools ensuring legal order (compliance, reporting, auditing, evidence-based governance).

Crucial for legal regulation is the realisation that "continuous interaction" in the Metaverse is legally significant not after the fact, but at the time of its implementation: it is then that there are risks of violation of privacy, security, discrimination and unlawful interference with the exercise of rights, which justifies the need for regulatory foresight and procedural formalisation of such interactions within the framework of information law and digital jurisdiction. Ignoring the evolutionary inheritance between IoT and Metaverse leads to fragmented legal regulation, while it is the systematic approach that allows building a holistic legal ontology of information relations in digital and immersive environments (Abdelzaher et al., 2023)[1].

2.2.2. Metaverse Blockchain (DLT): A "Trust Space" for Digital Jurisdictions.

Blockchain (in the broader class of DLT technologies) should be considered not as a "financial fashion", but as a legally relevant infrastructure that transfers part of trust from the level of institutional promises to the level of cryptographically secured protocoling. We are talking about the formation of a trust space in which the facts of digital interaction (transactions, access events, asset states, fulfilment of the terms of a smart contract) acquire increased evidence due to the immutability of the log, timestamps, and state coordination between network nodes. Conceptually, this makes it possible to bring the technological "truthfulness" of the record closer to the procedural "admissibility" of the evidence, provided that the legal regime is properly implemented. For the dissertation research, such a statement is fundamental, since Metaverse environments form polycentric digital ecosystems with high cross-borderality, where classical trust models (state register + territorial jurisdiction) often do not provide a full cycle: fact - proof - decision - execution.

The problem is that the blockchain infrastructure, despite its strong properties of immutability and synchronisation, is not a self-sufficient legal guarantor: it does not solve the issues of entity identification, legitimacy of network rules, responsibility for protocol updates, conflict of jurisdictions, and, most importantly, due process in disputes arising in the protocol environment. Hence the need to combine the technical properties of DLT with legal regimes (virtual assets, digital identity, compliance, data protection, law of evidence) so that on their basis it is possible to institutionalise electronic jurisdiction as a mechanism for legitimate dispute enforcement and enforcement of decisions.

To substantiate blockchain as an element of the Metaverse infrastructure, which acts as a "protocol layer of trust", and determine the legal consequences of its architectural options for evidence, liability and jurisdictional interoperability, we will analyse:

technical and legal characteristics of DLT (hashing, timestamp, consensus, finality) in the categories of evidence and accountability;

classifications (public/consortium/private; permissioned/unpermissioned) and their legal implications for access, liability and data protection regimes;

"compliance map" *technical function - legal function - legal regime / institution - risks - compliance safeguards*;

1 Abdelzaher, T., Caesar, M., Mendis, C., Nahrstedt, K., Srivastava, M., & Yu, M. (2023). Challenges in metaverse research: An Internet of Things perspective. In *Proceedings of the 2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*. 161–170. IEEE. https://doi.org/10.1109/MetaCom57706.2023.00042

two planes of blockchain application in the Metaverse: architecture (smart contracts, virtual assets, consensus) and procedures (verification/reputation/mutual recognition);

Comparative regulatory models and the Ukrainian context with a focus on the conditions of the possibility of digital jurisdiction.

Technical and legal characteristics of blockchain.

In a technical sense, blockchain is a distributed ledger where transactions are combined into blocks and blocks are linked together by cryptographic hash links; This chaining makes it possible to detect changes in past records, since modifying one block changes all subsequent hashes. Public standardised reviews (including NISTIR 8202) emphasise that "immutability" in blockchain is not metaphysical, but is the result of a combination of cryptography, network replication, and economic-organisational incentives.

The legal relevance of these components is manifested through logging as the technological equivalent of an event log with increased integrity. Hashing and timestamp (timestamp) make it possible to prove:

a) the fact of the existence of a certain set of data at a certain moment;

b) immutability of the record after inclusion in the circuit;

c) the sequence of events.

However, for procedural law, not only "integrity" is important, but also attribution: who exactly initiated the transaction, whether the key was compromised, whether the subject acted lawfully. That is why technical guarantees must be "supported" by legal regimes of digital identity, key management, incident response procedures, and standards for the admissibility of digital evidence. The key link is consensus — a way to reach agreement on the state of the registry (PoW, PoS, etc.). It is legally significant that consensus determines the level of finality (when a record is considered final), resistance to attacks, and a model of accountability for validators. This has a direct impact on evidence: in networks with "probabilistic finality" (typical for PoW), the procedural model must take into account the risk of reorganisations, while in networks with "deterministic finality" or in permissioned-DLT, this risk may be lower if there is a managed composition of validators and regulations for changing rules. From a dissertation perspective, this means: the evidentiary value of a blockchain record is always a function of the consensus architecture and governance model of the network, and not only of the fact of "writing to the blockchain".

It is also important to take into account protocol "trust vulnerabilities" that do not destroy cryptography but affect the fairness and predictability of outcomes: for example, MEV practices and rearranging transactions in blocks, which can cause hidden preferences in decentralised trading and smart contract execution. Academic research on the phenomenon of frontrunning in DEXs demonstrates that mempool transparency can generate systemic incentives to "intercept" profitable transactions (Daian et al., 2019)[1]. In the legal plane, this is transformed into the question: whether such behaviour is a tort/abuse of law in the protocol environment, what means of prevention should be

1 Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). *Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges* (arXiv:1904.05234v1). *arXiv.* https://arxiv.org/abs/1904.05234

recognised as appropriate, and how to qualify the damage caused by "algorithmic advantage".

The classification of networks into public/consortium/private and permissioned/unpermissioned is not a technical detail, but a design that determines the access regime, the circle of responsible persons and the possibility of applying regulatory supervision. In a permissioned network (with controlled access), it is easier to implement compliance (AML/KYC), role management, auditing, and procedural safeguards, but the risks of concentration of power and "privatisation" of rules increase. On the other hand, unauthorised networks increase openness and resistance to censorship, but complicate legal attribution, enforcement of decisions, and privacy protection. In view of the above, choosing the type of DLT for the Metaverse ecosystem is actually a choice of legal architecture: from "protocol publicity" to "managed trust" with distributed responsibility.

2.2.3. DTL-Metaverse matrix.

Matrix "infrastructure → legal regimes → trust → jurisdiction": blockchain becomes a legal infrastructure.

For the purposes of the dissertation, it is advisable to position blockchain as an infrastructure layer (Yaga et al., 2018)[1] that produces legal consequences through a chain of transitions:

Infrastructure: DLT as a legally relevant technical layer.

In the legal dimension, distributed ledger technology (DLT) should be considered not as an autonomous "regulator", but as an infrastructural layer of digital legal relations, which creates technical and procedural conditions for the occurrence, fixation and execution of legally significant actions. The key properties of DLT are logging (auditability), immutability of records, finality of transactions, tokenisation of objects, and the possibility of built-in execution of conditions through smart contracts. It is these properties that give the infrastructure features "legal relevance", since they correlate with the classical legal requirements for registers, evidence, forms of transactions and procedures for the fulfilment of obligations. At the same time, it is worth emphasising that DLT does not have its own regulatory force: it only materialises rules defined outside the protocol. – *In our opinion*, blockchain infrastructure is a form of technical and legal potential, which acquires legal significance solely through regulatory "connection" on the part of the law.

*Legal regimes: normative superstructure over protocol***.**

On the basis of DLT, heterogeneous but interrelated legal regimes are formed, which determine the permissible models of behaviour of participants and the legal consequences of their actions. First of all, we are talking about the regime of virtual assets as objects of civil and financial turnover, which require qualification from the standpoint of property, tax and regulatory law. No less significant is the digital identity regime, which ensures the attribution of actions to a specific subject and creates a basis for responsibility. Within the same infrastructure, compliance regimes (AML/KYC), admissibility, contractual and tort liability regimes, as well as protocol itself management regimes, in particular through decentralised models (DAOs), are formed. In view of the above, blockchain appears as

1 Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (NISTIR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

an environment of legal stratification, where different industry regimes are superimposed on a common technical basis, but do not merge into a single "techno-norm".

Trust: a combination of cryptography and procedural.

Trust in the blockchain environment is not reduced to the mathematical correctness of algorithms. It is formed as a synthesis of a cryptographic guarantee of data integrity and a legal guarantee of proceduralism. The first ensures the immutability and verifiability of records, the second determines who has the right to initiate changes, what procedures are used to make decisions, how disputes are resolved, and what are the mechanisms for restoring violated rights. Without legal formalisation of the procedures of management, appeal and responsibility, cryptographic trust remains "blind" and cannot perform a social and legal function. Let's assume that this is where the line between technological infrastructure and the legal order lies: trust does not arise in the code, but in the alignment of the code with legal procedures.

Jurisdiction: digital dispute enforcement in a protocol environment.

On the basis of the formed trust, it becomes possible for the emergence of digital jurisdiction as a specific form of exercising power and quasi-power functions in the digital environment. We are talking about the recognition of on-chain evidence, ensuring due process, procedural dispute resolution and enforcement of decisions both directly in the protocol (through smart contracts, asset freezes, automated execution) and through interoperable gateways with offline enforcement systems. In this context, digital jurisdiction appears not as a territorial, but as a functional-protocol category based on mutual recognition of procedures and results. Thus, digital jurisdiction is not a denial of the state legal order, but its new form of adaptation to decentralised digital ecosystems.

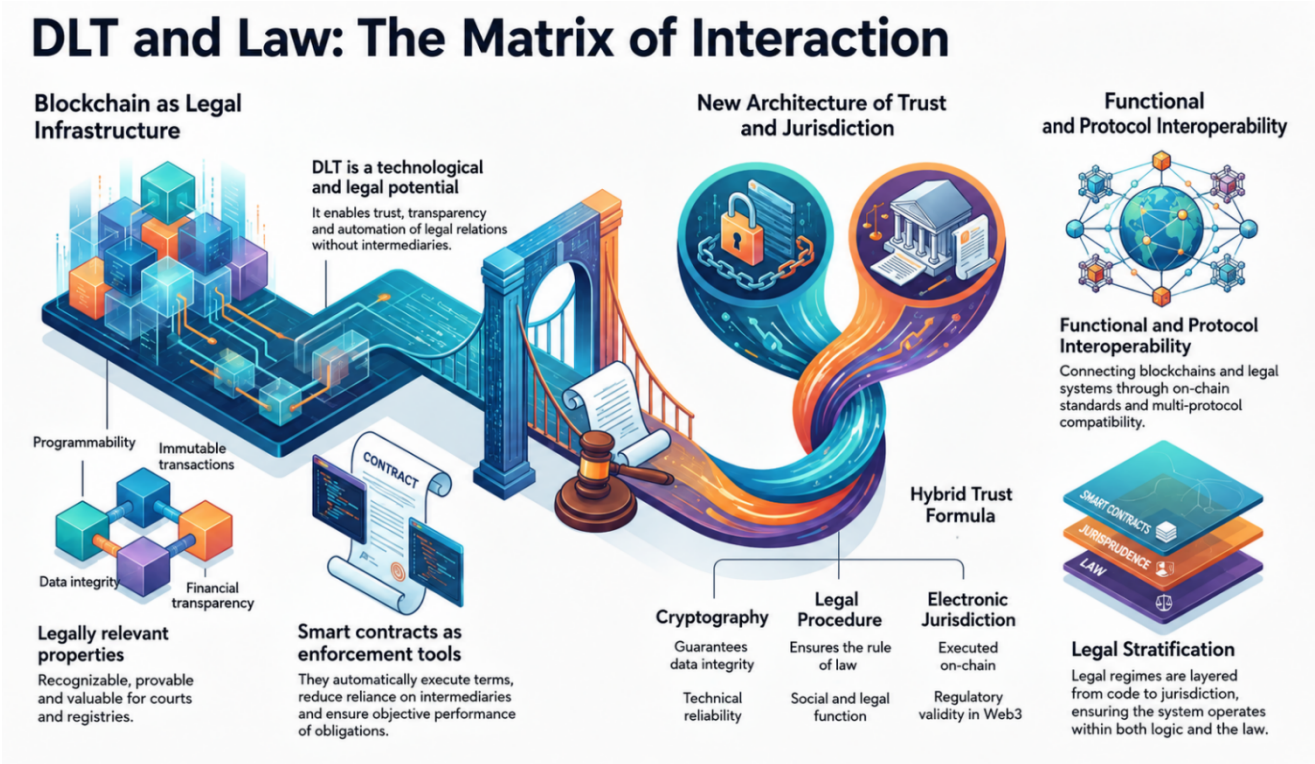


Figure 28. Metaverse: Interaction Matrix

Such a matrix demonstrates a fundamental thesis: blockchain does not "replace the law" and does not eliminate the need for it, but, on the contrary, radically actualises the law as a mechanism for legitimising the protocol (Figure 28). It is the law that determines the limits of the permissible autonomy of the code, the parameters of trust and the conditions of fair coercion. In this sense, e-jurisdiction appears not as a technical tool, but as a legal response to the infrastructural challenges of the Metaverse.

This is reflected in the "Compliance Map": Blockchain Technical Functions and Legal Implications (See Appendices. Table 3).

Note: the international DLT architecture standards and NIST review documents emphasise the need to distinguish between "technical immutability" and "organisational reliability" of the network as a condition for correct application in public administration and justice.

2.2.4. Blockchain in the Metaverse: Architecture and Legal Ontology.

In Metaverse environments, blockchain manifests itself in two interconnected planes.

1) The architectural plane encompasses tokenisation, smart contracts, and consensus mechanisms as the "supporting structure" of the economy and governance. Tokenization ensures the turnover of virtual assets and allows you to represent both property and functional rights (access, voting, use of digital objects). However, the legal fallacy lies in the identification of a "token" with a "right": a token is a technical carrier, while the legal title and boundaries of disposal are determined by the virtual asset regime, the treaty and the norms on the protection of the bona fide acquirer. That is why in the dissertation optics, tokenisation should be included in the legal ontology of the Metaverse: a list of objects, their attributes, ways of acquiring and losing rights, and title confirmation procedures.

A smart contract in the Metaverse should be described as a protocol form of commitment that combines legal will and machine execution. Its strength is in the predictability of execution, its weakness is in the fragility of the code and dependence on oracles. Hence the need for "algorithmic transparency" (in the minimal sense — the clarity of the execution logic for the parties and the controller) and procedural safeguards: the possibility of pause, error correction mechanisms, compensation, as well as determining the responsibility of the developer/operator for design defects.

2) The procedural plane includes protocols of interaction, verification, reputation and mutual recognition. The Metaverse is not only a "space of objects" but also a "space of interactions", where a significant part of conflicts is not reduced to a classic contract: blocking an avatar, removing a digital object, a "ban" in the environment, a dispute over the authorship of a digital artifact, tort damage from manipulation of algorithms. For such cases, blockchain provides basic evidence fabric — but only when the identity and events are described in a formalised way.

Here, the central concept is digital identity: who exactly is the bearer of rights and responsibilities in interaction in the Metaverse (person, avatar, digital person/agent, organisation). The standardisation of the DID approach at the W3C level demonstrates that digital identity can be decentralised and not require a single ledger, but it still requires trust mechanisms (verified attributes, revocations, key management policies). In this

regard, the blockchain in the Metaverse acts as a "register of states" and "register of powers", and law acts as a constructor of the legitimacy of these states and powers.

Separately, it is worth noting that trust procedures in the Metaverse can include reputational protocols and "social-protocol" verification models (anti-Sybil, confirmation of participation, rating based on behavioural events). Some scientific papers propose reputational mechanisms for network solutions (in particular, for the selection of relay nodes) as a way to increase reliability and reduce abuse; such approaches are useful for the dissertation as an example that "trust" can be protocol, but requires legal supervision so as not to become a discriminatory tool or a hidden punishment (Zhang et al., 2021)[1].

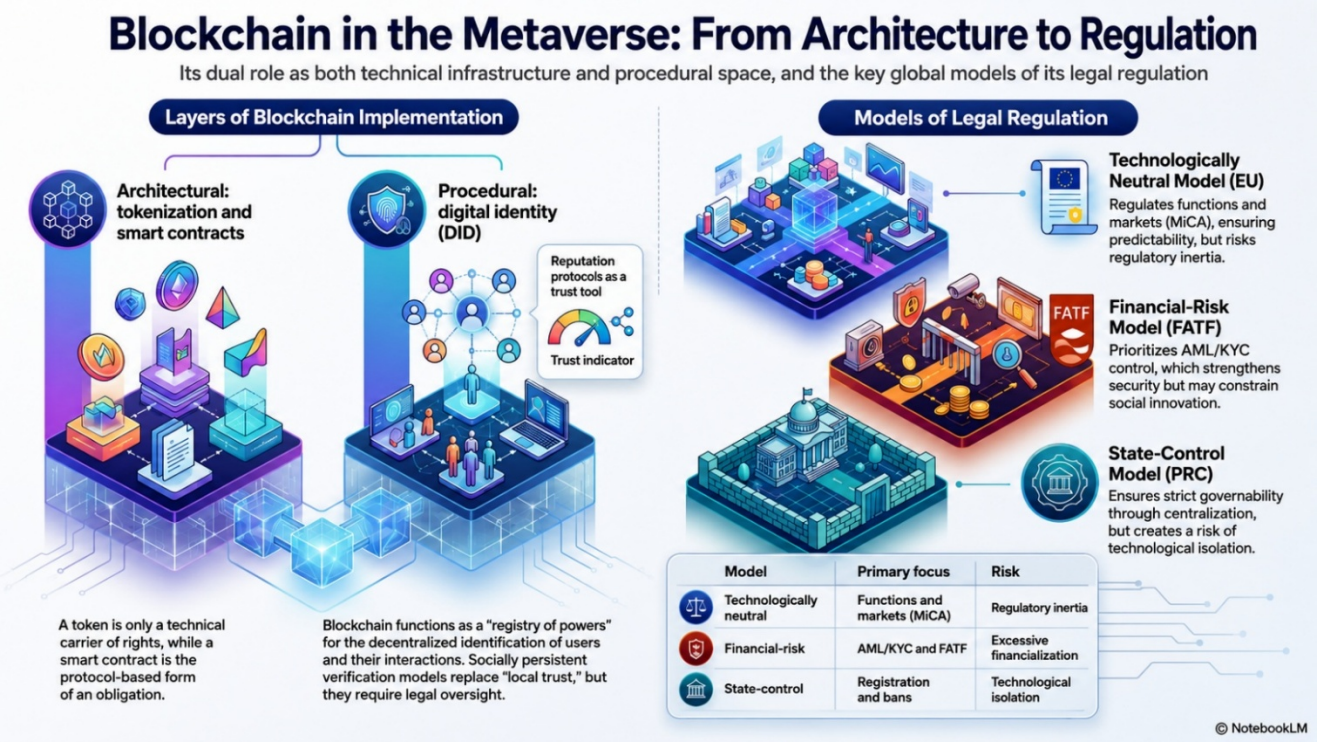


Figure 29. Metaverse: Blockchain.

Let us consider regulatory models as a comparative legal fragment (three approaches). Comparative analysis allows us to identify three basic models of legal regulation, which are differently "superimposed" on blockchain as an infrastructure (Figure 29).

1) Techno-neutral model. Its logic is not to "regulate blockchain as such," but to regulate specific functions and markets where DLT is the infrastructure: primarily the circulation of crypto assets, provider services, issuance requirements, and information disclosure. An example is the EU approach, where MiCA establishes a framework regulation of the crypto asset market, while DLT Pilot creates a mode for the experimental application of DLT in market infrastructure (Elliptic, 2021).[2] The advantage of the model is predictability and scalability; risk is "regulatory inertia", where technological

1 Zhang, M., et al. (2021). Accelerating transactions relay in blockchain networks via reputation. In *Proceedings of the 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS).* 1–10.IEEE. https://doi.org/10.1109/IWQOS52092.2021.9521324

2 Elliptic. (2021). *Regulation of cryptocurrency exchanges in Japan in 2021*. https://www.elliptic.co/blog/regulation-of-cryptocurrency-exchanges-in-japan

innovation is ahead of the categories of law (especially in Metaverse cases where assets are hybrid: property + functional access + data).

2) Financial and risk model. AML/KYC, VASP licensing, market surveillance, and consumer protection dominate here as priorities over the "Metaverse ontology." An influential reference point is the FATF standards for virtual assets and VASPs (in particular, the implementation of the Travel Rule), where the emphasis is on risk identification, tracing and control. The strength is the control of criminogenic practices; weak — potential narrowing of the space of innovation and excessive "financialisation" of any relationships in the Metaverse, even if they are mainly social and communicative in nature.

3) State-control model. It is focused on supplier registration, real-name modes, content restrictions, a strict ban on certain types of activities, and a centralised policy of "eligibility" of operations. An illustrative example is the PRC, where the regulations of 2021 qualify transactions with virtual currencies as illegal financial activities, restricting both domestic and offshore services aimed at residents. The advantage is controllability and speed of risk suppression; risk — narrowing of rights and freedoms, technological isolation and the emergence of shadow markets.

To show how these models are "decomposed" into specific jurisdictions, consider Summary Table 4.

2.2.5. Blockchain - Ukrainian context.

In Ukraine, Blockchain technologies have been used in public authorities since 2017. Thus, the Cabinet of Ministers of Ukraine approved the implementation of measures to implement the Blockchain data storage and protection system in the work of the Register of Property Rights to Real Estate and the SETAM electronic trading system of the Ministry of Justice of Ukraine. Ukraine, the NGO Transparency International Ukraine and Bitfuri Holding BV signed a Memorandum of Understanding and Cooperation for the purpose of forming and maintaining a land cadastre and other state registers based on Blockchain technology, as well as developing a methodology for using Blockchain in the public sector. Thus, the updated State Land Cadastre has already been formed using Blockchain technology. The Law of Ukraine "On Virtual Assets" was also adopted, the purpose of which is to regulate legal relations regarding the circulation, storage, possession, use and transactions with cryptocurrency in Ukraine (Law of Ukraine "On Virtual Assets", (2022)[1].

At the same time, in accordance with the provisions of the Concept for the Development of the Digital Economy and Society of Ukraine for 2018-2020, which was approved by the Cabinet of Ministers of Ukraine dated January 17, 2018 No. 67 (Cabinet of Ministers of Ukraine, 2018)[2], blockchain was defined as a software and computer algorithm of a decentralised public or private register or database, the functioning of

1 Pro virtualni aktyvy [On virtual assets], Law of Ukraine №. 2074-IX (2022). https://zakon.rada.gov.ua/laws/show/2074-20#Text

2 Cabinet of Ministers of Ukraine. (2018, January 17). *Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018–2020 roky ta zatverdzhennia planu zakhodiv shchodo ii realizatsii* [On approval of the Concept for the development of the digital economy and society of Ukraine for 2018–2020 and approval of the action plan for its implementation] (Decree No. 67-r). https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

which is ensured by the interaction of a peer-to-peer network via the Internet, or in any other way that guarantees proper cryptographic protection of all records, transactions conducted using the appropriate technology.

At the same time, the national regulatory framework is characterised by frequent examples of the adoption of narrow-profile laws, which cause a situation in which even experts are not able to clearly answer the question of which norm should be applied in a particular case, and there is unsystematic development of legislation in general, including inconsistencies between their individual norms. Overcoming conflicts of legislation is an important condition for achieving its consistency. One of the problems is also non-compliance with technical and legal requirements for law-making activities (Omelchenko, 2021)[1]. In addition, there is a dilemma of the legitimacy of regulatory documents, which is that according to generally accepted practice, by-laws can only interpret existing laws and cannot create new rights and obligations. Instead, there is a widespread practice of issuing various types of administrative documents, explanations, instructions, recommendations that contain different versions of certain norms, which creates a "legal conflict". These regulatory documents are often a reaction to certain incidents in the information sphere, as an attempt to temporarily regulate processes that do not have legislative regulation.

The spread of an unqualified and unsystematic approach to the sphere of legal regulation in a significant number of cases gives rise to the emergence of a "legislative virus" (Kyrychko, 2016; Kyrychko, 2021)[2,3], and leads to "aberration of regulatory information" (Korzh, n.d.)[4]. In general, this state leads to inconsistency and contradiction of criminal law and other prescriptions, violation of the principle of legal certainty as an integral element of the rule of law, and results in complications in understanding the content of the norm and qualification of certain actions in the practice of law enforcement. Overcoming these negative consequences in many cases requires "scientific divination" (Radutnyi, 2016) (Tao, 2019)[5] – a forced method of interpreting modern regulations, which consists in finding an incomprehensible craft and a higher spirit manifested in legislative decisions of people gathered in a bunch of random people for a particular case, interpreting the results of their rule-making activities in a systematic connection with already existing norms, trying to eliminate the identified contradictions with their own scientific forces.

---

1 Omelchenko, A. V. (2021). Zakonodavstvo Ukrainy u sferi tsyfrovoi transformatsii: stan rozvytku ta perspektyvy systematyzatsii [Legislation of Ukraine in the field of digital transformation: State of development and prospects of systematization]. *Juris Europensis Scientia, 6,* 60–63. https://doi.org/10.32837/chern.v0i6

2 Kirychko, V. M. (2016). Zakonodavchyi virus u systemi KK Ukrainy: vyznachennia i aktualizatsiia problemy na prykladi st. 368-2 KK "Nezakonne zbahachennia" [Legislative virus in the system of the Criminal Code of Ukraine: Definition and actualization of the problem on the example of Art. 368-2 of the Criminal Code "Illicit Enrichment"]. *Problemy zakonnosti* [Problems of Legality], *133*, 142–151.

3 Kirychko, V. M. (2021). Pro systemni zakonodavchi virusy i sotsialni zasady stvorennia novoi systemy Kryminalnoho kodeksu Ukrainy [On systemic legislative viruses and social foundations for creating a new system of the Criminal Code of Ukraine]. *Visnyk asotsiatsii kryminalnoho prava Ukrainy* [Herald of the Association of Criminal Law of Ukraine], *2*(16), 1–26. https://vakp.nlu.edu.ua/issue/view/14857

4 Korzh, I. F. (2021). Aberatsiia normatyvno-pravovoi informatsii [Aberration of regulatory and legal information]. *Informatsiia i pravo* [Information and Law], *1*(36), 9–17.

5 Radutnyi, O. E. (2016). Stan informatsiino-zakonodavchoi diialnosti na prykladi Kryminalnoho kodeksu Ukrainy [The state of information and legislative activity on the example of the Criminal Code of Ukraine]. *Informatsiia i pravo* [Information and Law], *3*(18), 58–66. https://doi.org/10.37750/2616-6798.2016.3(18).272969

With blockchain technology and smart contracts, many societal processes can be digitised and translated into simple and deterministic code-based rules that will be automatically enforced by the underlying blockchain network, using technology and codes to make sure people comply with the law. By transforming parts of the law into technical regulations, legal provisions can be provided with a basic technical structure, reducing the need for supervision and continuous enforcement[1].

Taking into account the need to transform "analog" legislation in accordance with the development of digital technologies, we offer the author's definition of the term blockchain:

«Blockchain is an electronic decentralised public register (database) distributed in any public electronic data transmission network, which contains information about actions with any electronic transactions recorded using an immutable cryptographic signature."

It should be noted that the Ukrainian regulatory framework of the market of virtual assets and related services is in the completion phase, where the key node is tax and institutional setup. The Law of Ukraine "On Virtual Assets" (No. 2074-IX) was adopted in 2022, but its enactment was associated with the adoption of amendments to the Tax Code; In 2025, steps were publicly communicated to promote relevant draft laws/taxation models and launch the market in 2026-2027. For even with incomplete implementation of the special regime of virtual assets, Ukraine already operates with a developed field of e-governance and electronic registers, as well as mechanisms for electronic identification/trust services.

Therefore, blockchain infrastructure can be integrated into the Ukrainian legal field in two modes:

- as an infrastructure for the circulation of virtual assets (market, supervision, AML);
- as an evidentiary recording infrastructure for certain public law procedures (event registers, fixation of statuses, control of the immutability of records).

1 Tao, U. (2019). Blockchain regulation: Dilemma and way out. *Legal Journal*. https://www.fxcxw.org.cn/dyna/content.php?id=12674

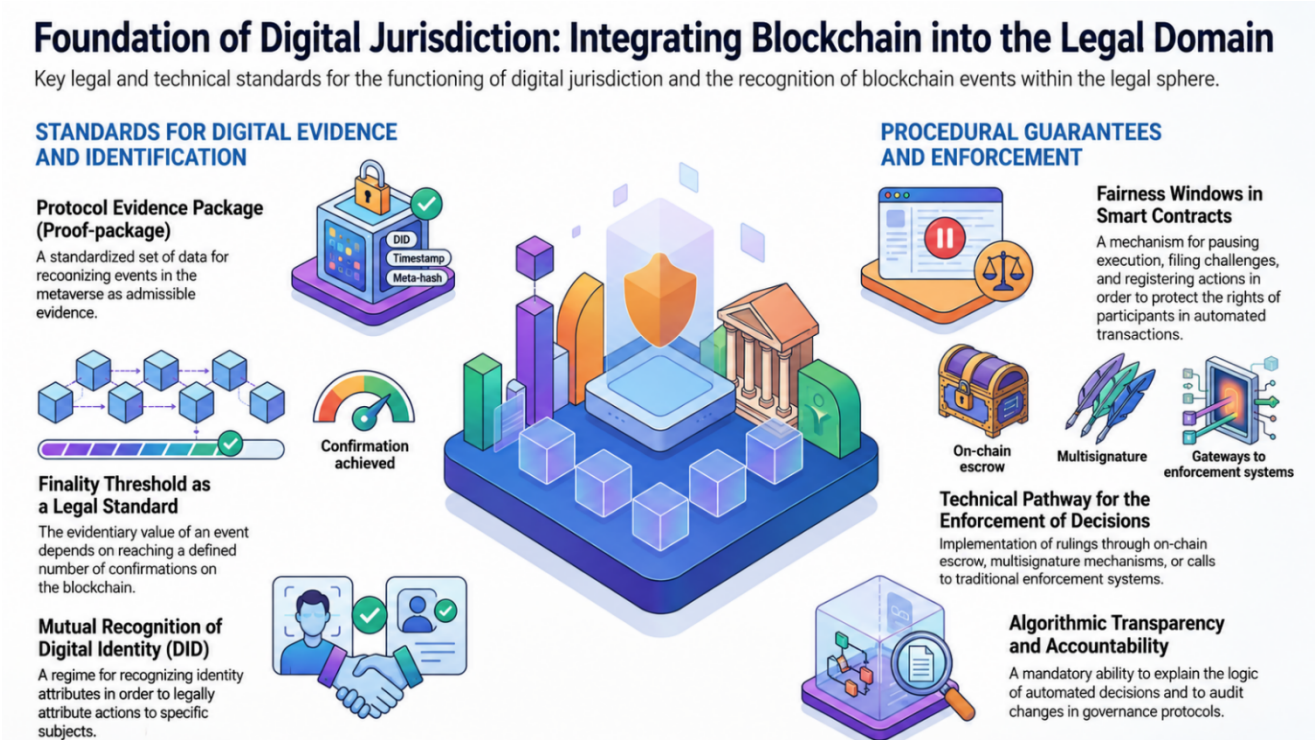


Figure 30. Metaverse: blockchain as the foundation of digital jurisdiction.

The second mode forms normative and procedural "pillars" that directly pass into the foundation of digital jurisdiction (evidence, due process, mutual recognition, enforcement of decisions in a protocol environment) (Figure 30), namely:

1) Protocol evidence package. For events in the Metaverse, a minimum "proof-package" must be defined: data hash ID, timestamp, block/transaction reference, source metadata, and rules for reproducing the original source. This creates a standardised object for admissibility in the digital jurisdiction procedure.
2) Finality as a procedural threshold. The evidentiary value of the on-chain event must depend on the achievement of a defined finality threshold (number of confirmations/deterministic finality in permissioned-DLT). The relevant threshold is a procedural standard and should be enshrined in the rules of electronic justice/arbitration.
3) Due process in smart contract execution. Automated execution (smart contract) should allow for procedural "windows of fairness": a mechanism for appealing, suspension of execution in a dispute, and a procedure for restoring the disturbed state (restitution/compensation). Otherwise, protocol coercion turns into extra-procedural coercion.
4) Mutual recognition of digital identity. Electronic jurisdiction in the Metaverse requires a regime of mutual recognition of digital identity attributes (DID/VC or equivalents) in order to attribute actions to entities and establish jurisdictional links (place of service provision, residency, provider status).
5) Thesis on protocol execution of decisions. A digital jurisdiction solution must have a technical execution path: either through on-chain escrow/multisignature or through an interoperable gateway to off-chain actuators. Without an enforcement mechanism, jurisdiction loses its practical meaning.
6) Responsibility for governance and upgrades. Protocol changes (forks, smart contract upgrades, access rule updates) must fall under procedural standards:

notifications, voting/legitimation, auditing, the possibility of appeal. This is the sphere of decentralised governance and at the same time the sphere of legal responsibility for the consequences of upgrades.

7) Algorithmic transparency as a condition of trust. For disputes in the protocol environment, there should be a minimum standard of algorithmic transparency: the ability to explain the logic of key automated decisions (sanctions, blocking, write-offs, reputational consequences). Without this, the due process becomes declarative, and the "space of trust" becomes fragile.
8) Legal interoperability and collisions. In transnational Metaverse environments, conflict of laws rules are necessary for mutual recognition: what evidentiary regime applies, which jurisdiction is competent, how decisions are recognised, how compliance requirements (AML/KYC) are agreed between providers. Protocol interoperability must be complemented by legal interoperability, otherwise there will be an "island" trust without jurisdictional force.

Thus, blockchain (DLT) within the Metaverse paradigm appears not as an autonomous substitute for law, but as an infrastructure layer that creates the technical prerequisites of the trust space due to the immutability of the event log, finality of states, and protocol execution of rules, while leaving open the question of legal guarantees of procedurality and legitimation, since its legal relevance is concentrated primarily in the planes of evidence, attributability, and accountability, which directly depend on architecture consensus, access modes, and governance models of the respective networks. In this context, the classifications public/consortium/private and permissioned/unpermissioned acquire not a purely technical, but a normative meaning, since they determine compliance parameters, the distribution of responsibilities, the level of data protection and the ability to enforce decisions, i.e. they form the "jurisdictional suitability" of the digital environment.

In the Metaverse, blockchain functions both as an architecture (through virtual assets and smart contracts) and as a procedure (through verification, reputation, and mutual recognition mechanisms), forming a legal ontology of objects and entities, centred on digital identity as a key node for the attribution of rights and obligations.

Comparative legal analysis shows the existence of at least three dominant regulatory models — techno-neutral, financial-risk, and state-controlled — each of which balances innovative development and human rights protection in its own way, while global AML/FATF standards and regional regimes (EU, UK, Singapore) already set mandatory compliance frameworks that are inevitably projected onto Metaverse platforms.

The Ukrainian legal context is at the stage of institutional formation of virtual assets and taxation regimes, which opens a "window of opportunity" for laying from the very beginning procedural standards of evidence and implementation as the foundation of the future digital jurisdiction.

It is advisable to focus further research on on-chain evidence admissibility standards, due process models in smart contract execution, jurisdictional maturity models for protocol environments, and mechanisms for mutual recognition of digital identity and decisions in multi-entity Metaverses, since blockchain in the legal framework should be fixed precisely as an infrastructure that forces the right to become protocol, and digital jurisdiction as a procedural way to transform protocol trust into a legal one legitimate.

2.2.6. Blockchain, IoT and AI - the basis of digital jurisdiction.

To solve the problem of providing fast blockchain in the Metaverse (Alja'afreh et al., 2023; Mishra et al., 2022)[1, 2], it is proposed to combine the blockchain structure with the architecture of IoT (Internet of Things, Comprehensive Internet – English. Internet of Things, IoT, Internet of Everythings, IoE – the concept of a network consisting of physical devices interconnected at the software and hardware levels, which allows the transfer and exchange of data between the physical world and computer systems in automatic mode, through the use of standard communication protocols) by creating a hierarchical structure for storing metadata, where key data will be on cloud services, blocks with the latest changes will be stored on IoT devices (Nalbant & Uyanik, 2022)[3]. For example, it is proposed to validate the block header only when necessary, which will reduce the interaction time between Ethereum-based blockchains (Miyaguchi, 2022) [4], or change the traditional linear structure of blockchains to a directed acyclic graph (DAG) structure (Wang et al., 2019)[5], as well as apply the UTXO-based virtual channel protocol, which is compatible with almost all cryptocurrencies (Frauenthaler et al., 2020) [6], or the Repulay protocol and others.

Today, blockchains related to Ethereum and Bitcoin are used in the Metaverse. Blockchain authentication in the Metaverse and its use provides access to virtual asset auctions, ownership, development, and lease of e-Land, creation and sale of e-items, e-real estate-related activities, cryptocurrency investing, and more (Gadekallu et al., 2022)[7].

Currently, two types of blockchain are used in the Metaverse: for the formation of architecture (smart contracts (Yang et al., 2019)[8]), consensus mechanisms (Aumayr et al., 2021)[9], cryptocurrency) and the formation of procedures (Repulay protocol (Daian et al., 2019)[10], probabilistic blockchain (Duong et al., 2018)[11], alliance with reputation (Zhang

1 Alja'afreh, M., Alouneh, S., Obaidat, M., Karime, A., & Elsaddik, A. (2023). Metaverse through blockchain and intelligent networking: A comprehensive survey. In *Proceedings of the 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)*. 426–439. IEEE. https://doi.org/10.1109/BCCA58897.2023.10338851

2 Mishra, S., Arora, H., Parakh, G., & Khandelwal, J. (2022). Contribution of blockchain in development of metaverse. In *Proceedings of the 2022 7th International Conference on Communication and Electronics Systems (ICCES)* (pp. 845–850). IEEE. https://doi.org/10.1109/ICCES54183.2022.983598

3 Nalbant, K. G., & Uyanik, Ş. (2022). A look at the new humanity: Metaverse and metahuman. *International Journal of Computers*, *7*, 7–13. https://www.iaras.org/iaras/journals/ijc

4 Miyaguchi, A. (2022). *How can blockchain principles help improve ESG systems?* https://www.weforum.org/agenda/2022/03/blockchain-principles-improve-esg-systems/

5 Wang, G., Shi, Z., Nixon, M., & Han, S. (2019). ChainSplitter: Towards blockchain-based industrial IoT architecture for supporting hierarchical storage. In *Proceedings of the IEEE International Conference on Blockchain (Blockchain'19)* (pp. 166–175). https://eprint.iacr.org/2019/1138.pdf

6 Frauenthaler, P., Sigwart, M., Spanring, C., Sober, M., & Schulte, S. (2020). ETH relay: A cost-efficient relay for Ethereum-based blockchains. In *2020 IEEE International Conference on Blockchain (Blockchain)* (pp. 204–213). IEEE. https://doi.org/10.1109/Blockchain50366.2020.00033

7 Gadekallu, T., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, V., Costa, D., & Liyanage, M. (2022). Blockchain for the metaverse: A review. *arXiv.* https://doi.org/10.48550/arXiv.2203.09738.

8 Yang, S., Chen, Z., Cui, L., Xu, M., Ming, Z., & Xu, K. (2019). CoDAG: An efficient and compacted DAG-based blockchain protocol. In *Proceedings of the IEEE International Conference on Blockchain*.. 314–318. https://ieeexplore.ieee.org/document/8946190

(Aumayr et al., 2021)10 Aumayr, L., Ersoy, O., Erwig, A., Faust, S., Riahi, S., Hostáková, K., Maffei, M., & Moreno-Sanchez, P. (2021). Bitcoin-compatible virtual channels. In *Proceedings of the IEEE Symposium on Security and Privacy*. 901–918. https://publik.tuwien.ac.at/files/publik_292507.pdf

10 Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. *arXiv*. https://doi.org/10.48550/arXiv.1904.05234.

11 Duong, T., Chepurnoy, A., Fan, L., & Zhou, H.-S. (2018). TwinsCoin. In *Proceedings of the 2nd ACM Workshop on*

et al., 2021)[1]), Blochchain Meet IoT (Salman et al., 2019)[2] , quick certificate check (Malik et al., 2019)[3]).

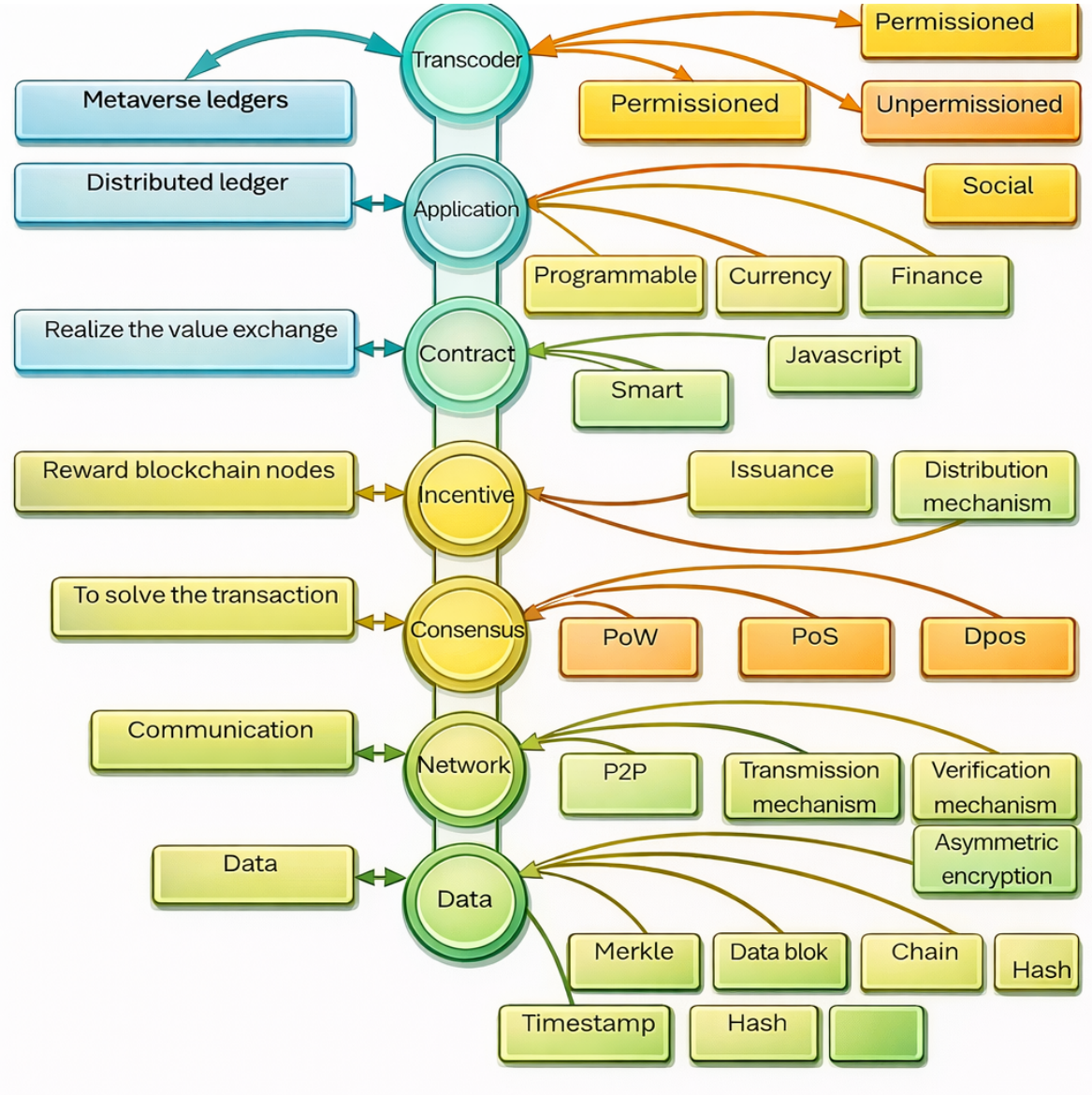


Figure 31. Metaverse: Typical Blockchain Architecture

Blockchains can store and provide access to a variety of data for artificial intelligence, including datasets, algorithms, and computing power (Novo, 2018)[4]. It is

Blockchains, Cryptocurrencies, and Contracts 1–13. ACM. https://doi.org/10.1145/3205230.3205233.

1 Zhang, M., Cheng, Y., Deng, X., Wang, B., Xie, J., Yang, Y., & Zhang, J. (2021). Accelerating transactions relay in blockchain networks via reputation. In *Proceedings of the IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)*.1–10. EEE. https://doi.org/10.1109/IWQOS52092.2021.9521324

2 Salman, S., Jain, R., & Gupta, L. (2019). A reputation management framework for knowledge-based and probabilistic blockchains. In *Proceedings of the IEEE International Conference on Blockchain*. 520–527. IEEE. https://doi.org/10.1109/Blockchain.2019.00078

3 Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). Trustchain: Trust management in blockchain and IoT supported supply chains. In *Proceedings of the IEEE International Conference on Blockchain*. 184–193. IEEE. https://doi.org/10.1109/Blockchain.2019.00032

4 Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, *5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239

decentralised AI and blockchain that allows you to process and perform analytics or predict decisions without the intervention of trusted third parties (Figure 31).

Regulation of blockchain technologies at the present stage of development of social relations with the use of information and communication technologies and adaptation to the results of the development of analog law focuses on streamlining the problem of legal regulation of digital currencies (ICO, Initial coin offering) based on blockchain (Truong et al., 2023)[1].

Today, there are several views on the regulation of blockchain-based digital currencies:

cryptocurrencies are electronic representations of value, not financial products (Wang et al., 2020; Yang et al., 2022)[2,3];

cryptocurrencies are considered financial instruments in the form of crypto assets (Kim, 2018)[4];

cryptocurrencies are property (Zhou, 2018; Blockchain: Legal & Regulatory Guidance, n.d.)[5,6];

cryptocurrencies are legal tender (Kenton & Murry, n.d.; Kagan et al., n.d.)[7, 8].

Currently, blockchain technologies are mainly used to create and develop electronic products and services that require maximum trust in the data stored and processed (Aks et al., 2022).[9] For example, this approach takes place in health care technologies, in the field of financial securities, accounting and auditing, public and administrative services, geodesy and land management, judicial systems, etc. These and other areas and areas of application of blockchain technologies are in constant evolution and in this regard require due attention from legal theorists and government agencies (Rajawat et al., 2023).[10]

An analysis of the legislation of different states indicates that legal regulation in general is aimed at improving social relations that arise on the basis of or in connection

1 Truong, V., Le, L., & Niyato, D. (2023). Blockchain meets metaverse and digital asset management: A comprehensive survey. *IEEE Access*, 11, 26258–26288. https://doi.org/10.1109/ACCESS.2023.3257029.

2 Wang, M., Qian, C., Li, X., Shi, S., & Chen, S. (2020). Collaborative validation of public-key certificates for IoT by distributed caching. *IEEE/ACM Transactions on Networking*, *29*(1), 92–105. https://doi.org/10.1109/INFOCOM.2019.8737423

3 Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., & Zheng, Z. (2022). Fusing blockchain and AI with metaverse: A survey. *arXiv*. https://doi.org/10.48550/arXiv.2201.03201.

4 Kim, Y.-c. (2018). Korea to allow ICOs with new regulations. *The Korea Times*. Retrieved from https://www.koreatimes.co.kr/www/biz/2018/04/367_245242.html

5 Zhou, Z. (2018). *Overview of South Korea's virtual currency legal policy (First Edition).* Zhihu. Retrieved September 11, 2022, https://zhuanlan.zhihu.com/p/46746556

6 Blockchain: Legal & Regulatory Guidance (2nd ed.). (n.d.). Latham & Watkins. Retrieved September 17, 2022, https://www.lw.com/admin/upload/SiteAttachments/Blockchain%20Legal%20%20Regulatory%20Guidance%20-%20Section%20Edition%2014%20-%20Latham%20authored.pdf

7 Kenton, W., & Murry, C. (n.d.). *Financial Conduct Authority (UK) (FCA).* Investopedia. Retrieved September 11, 2022, from https://www.investopedia.com/terms/f/financial-conduct-authority-uk-fca.asp

8Kagan, J., Cheng, M., & Kvilhaug, S. (n.d.). *Financial Services Agency (FSA).* Investopedia. Retrieved September 11, 2022, f https://www.investopedia.com/terms/f/financial-services-agency-fsa.as

9 Aks, S., Karmila, M., Givan, B., Hendratna, G., Setiawan, H., Putra, A., Winarno, S., Kurniawan, T., Simorangkir, Y., Taufiq, R., & Herawaty, M. (2022). A review of blockchain for security data privacy with metaverse. *2022 International Conference on ICT for Smart Society (ICISS),* 1–5. https://doi.org/10.1109/ICISS55894.2022.9915055.

10 Rajawat, A. S., et al. (2023). Enhancing security and scalability of metaverse with blockchain-based consensus mechanisms. *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1–6. https://doi.org/10.1109/ECAI58194.2023.1019403.

with the use of electronic products created on the basis of blockchain technology (Ud Din et al., 2023) (Ud Din et al., 2023)[1].

There are quite a few legislative acts directly aimed at regulating blockchain technologies, while the current regulations are aimed not at legal or technical-legal regulation, but mostly at technological regulation.

At the same time, blockchain is an electronic technology that encompasses electronic devices, data transmission networks, the Internet, data identification and storage technologies, cryptographic protection, cybersecurity, and other information technologies. In fact, it is possible to apply the norms of various branches of law, including information law, to blockchain (Elsadig et al., 2024)[2]. However, the rapid development of social relations significantly outstrips the state of legal regulation by the norms of analog law, and this creates a significant imbalance. The problem of the lack of legal regulation of blockchain at the level of laws leads to the creation of highly specialised regulatory systems and the generation of local by-laws by them , such as draft regulations for comments, recommendations, industry standards and norms, orders and instructions of individual enterprises and institutions, etc.

In analog legislation, the norms governing relations in the field of information and communication technologies and information law are historically "dispersed" across different branches of law, individual laws and regulations.

2.3. Decentralized Autonomous Organizations (DAOs) as the Newest Form of Digital Self-Government: Legal Nature and Functions

2.3.1. Decentralized Autonomous Organization (DAO) in the classical sense

A Decentralized Autonomous Organization (DAO) in the classical sense is a form of digital organisation based on the use of distributed ledger technologies (DLT, primarily blockchain), where the rules for functioning, management, and decision-making are formalised in the form of smart contracts and executed automatically without the need for a centralised governing body. A DAO functions as a protocol-defined system in which the coordination of participants' actions is ensured by code rather than a hierarchical administrative structure.

From an organisational and legal point of view, a DAO is an unconventional form of collective action that combines elements of an organisation, a contract, and a technical platform. It does not necessarily have the status of a legal entity in the classical sense, and its "will" and "decisions" are implemented through pre-programmed algorithmic rules. It is this feature that determines the autonomy of DAOs: after the deployment of smart contracts, their execution occurs automatically and predictably, without discretionary intervention of individuals.

A key feature of a DAO is the decentralisation of governance, which means that there is no single centre of control or management. Decisions within a DAO are made

1 Ud Din, I., Awan, K. A., Almogren, A., & Rodrigues, J. J. P. C. (2023). Integration of IoT and blockchain for decentralized management and ownership in the metaverse. *International Journal of Communication Systems*. https://doi.org/10.1002/dac.5612

2 Elsadig, M., Alohali, M. A., Ibrahim, A. O., & Abulfaraj, A. W. (2024). The Role of Blockchain in the Metaverse: Concepts, Taxonomy, Recent Advances, Enabling Technologies, and Open Inquiry Questions. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3367014

collectively by its participants — usually through voting or other forms of consensus enshrined in smart contracts. This approach is opposed to traditional corporate models, where managerial power is concentrated in management bodies or in a narrow circle of officials.

The second defining element of a DAO is algorithmic autonomy. The rules of the organisation's functioning — the procedure for decision-making, the allocation of resources, the conditions of participation, the mechanisms of incentives and sanctions — are fixed in the code of smart contracts. This ensures predictability and formal equality of the participants, since the implementation of the rules does not depend on the human factor, political expediency or situational decisions of the management.

The third characteristic feature of DAOs is transparency and verifiability. Since smart contracts and transactions are usually hosted on a public or consortium blockchain, any interested participant can check the organisation's operating rules, decision history, and resource movement. In this sense, the DAO implements the principle of "code as law", where the norm of behaviour exists in the form of program code open to verification.

From a socio-economic point of view, DAOs are seen as a tool for coordinating communities in the digital environment, allowing for collective management of resources, projects, or common interests without creating traditional institutions. DAO participants can have different status and scope of influence, which is often determined by the token model, reputation mechanisms, or formalised roles.

2.3.2. The legal nature of the DAO.

In legal doctrine, a DAO is usually defined as a technically determined organisational form at the intersection of private law, contractual relations, and digital technologies. At the same time, it should be emphasised that there is no universal, legally enshrined definition of DAO today: most definitions are doctrinal or descriptive in nature. Therefore, attention, information does not have reliable confirmation in the form of a single mandatory normative definition, and the given interpretation reflects the established scientific and technical and legal position.

Let's form the author's definition - A decentralised autonomous organisation (DAO) is an algorithmically and legally controlled digital ecosystem system of organised interaction of subjects used for automated support of legal procedures based on predetermined protocol rules enshrined in digital code, decision-making, accounting, resource allocation or interaction of participants, the functioning of which is based on smart contracts and does not provide for centralised administrative control or the exercise of power without a separate legal mandate.

In the context of the Metaverse, DAOs are seen as local, corporate, or national "digital jurisdictions" and the underlying mechanism of decentralised platform governance, contrasted with the monopolies of centralised Metaverse platforms. Modern scientific research describes the five-tier architecture of DAOs and forms the main goals of DAOs in the Metaverse: management of virtual property and markets (digital land, digital buildings, NFTs), decentralised platform/world governance (rules, updates, budgets), and coordination of economic activity (energy, transportation, gaming, DeFi ecosystems).

Decentralized Autonomous Organizations (DAOs) represent a non-standard new phenomenon in the development of organisational and legal forms, formed at the intersection of private law, information technology and the economy of digital platforms. Their emergence is due to the evolution of decentralised distributed ledger technologies and the desire to minimise the role of centralised intermediaries in the processes of management, coordination and distribution of resources. Unlike traditional legal entities, DAOs are not based on a classic corporate hierarchy, statutory governing bodies, or centralised administrative apparatus, which is characteristic of corporate and quasi-corporate models of organisation.

The functioning of the DAO is ensured by a set of smart contracts placed in a distributed ledger, which perform not only a technical but also a regulatory function, determining the procedure for decision-making, management of common assets, distribution of financial resources, and the implementation of the collective will of participants. From a legal point of view, such smart contracts act as software-fixed rules of conduct that act automatically and directly, without the need for human administrator intervention. This fundamentally distinguishes DAOs from traditional forms of organisation, in which regulatory regulation is carried out mainly through constituent documents, corporate acts, and expressions of will of governing bodies.

From a legal point of view, it is advisable to consider decentralised autonomous organisations as *a sui generis organisational entity*, which cannot be fully identified either with a legal entity in the classical sense, or with traditional forms of contractual or corporate associations. This approach is due to the fact that DAOs do not have constituent documents in the usual sense for private law, do not imply the presence of permanent governing bodies and do not function on the basis of hierarchical distribution of powers.

The normative behaviour of DAOs is determined primarily by the program code of smart contracts, which performs a regulatory function similar to that of internal regulations or statutes in traditional organisational and legal forms. Such a code fixes the rules for the entry and exit of participants, the procedure for making collective decisions, mechanisms for managing common assets and the conditions for the distribution of resources, and its implementation is automated and mandatory.

In the doctrine of digital law, this phenomenon is called according to which algorithmically fixed rules of conduct acquire a quasi-normative character and actually perform the function of private regulation: Lex cryptographia is a doctrinal term used in modern legal and interdisciplinary science to denote a set of rules of conduct, procedures and restrictions that are formed and provided by cryptographic algorithms, protocols and program code, rather than traditional ones normative legal acts of the state. In the literal sense, *lex cryptographia* means "the law of cryptography" or "the law embedded in cryptography", emphasising the idea that regulatory power comes from the technical architecture of the system, and not from the will of the legislator. Unlike classical rules of law, such rules are not based on state coercion, but are provided by the technical impossibility of violating them or deviating from a given algorithm. This has direct implications for the role of the state in regulating decentralised digital organisations.

DAOs combine the features of a multilateral civil law contract, a digital platform, a self-regulatory organisation, and an automated asset management system, which indicates their complex and multi-level legal nature. As a multilateral agreement, DAOs are based

on participants voluntarily joining predetermined rules fixed in smart contracts. As a digital platform, they provide a technical infrastructure to coordinate the interaction of an indeterminate circle of people in a decentralised environment. As a self-regulatory organisation, DAOs form their own decision-making and internal control mechanisms without the involvement of government or corporate authorities. Finally, as an automated asset management system, they dispose of financial and other digital resources based on pre-laid algorithms.

Such hybridity significantly complicates the legal qualification of DAOs within the traditional institutions of private and public law, since none of the existing organisational and legal forms fully covers all the functional characteristics of these entities. As a result, there is a need for a special regulatory approach that would take into account both the contractual nature of the relationship between DAO participants and the publicly significant aspects of their activities related to the management of shared resources, the protection of the rights of third parties, and ensuring law and order in the digital environment.

2.3.3. Legal personality and legal responsibility of the DAO.

The problem of legal personality is central and system-forming for the legal analysis of decentralised autonomous organisations. In most modern legal systems, DAOs are not recognised as independent subjects of law in the classical sense, which significantly complicates or completely makes it impossible for them to fully participate in civil turnover, in particular, concluding contracts, acquiring property and non-property rights, speaking in court, as well as exercising responsibility for violation of obligations.

In the absence of legal personality, DAOs are actually in a state of normative uncertainty, as a result of which there is a problem of identifying the holder of rights and obligations. In such conditions, legal responsibility for actions committed within the framework of the functioning of the DAO may be assigned to individuals or legal entities that directly or indirectly affect its activities. Such individuals include, in particular, smart contract developers as authors of algorithmic rules, active governance participants initiating and supporting governance decisions, as well as token holders who own a significant amount of votes and actually exert a decisive influence on the results of decentralised voting.

Such an approach, however, contradicts the basic principles of legal certainty and limited liability, since DAO participants are often not aware of the degree of their own legal risk, and the mechanisms for bringing them to justice do not have a clear regulatory framework. This actualises the need for the formation of special legal structures that would make it possible to clearly distinguish the responsibility of the DAO as an organisational entity from the responsibility of individual participants, as well as to determine the criteria for the occurrence of joint and several or subsidiary liability in cases of damage or violation of the rights of third parties.

From a legal point of view, the situation is especially difficult when a decentralised autonomous organisation operates in a cross-border environment, and its participants, developers and beneficiaries are located in different jurisdictions or cannot be uniquely identified at all. Under such conditions, a complex problem arises of determining the

applicable law, the jurisdiction of the court, as well as the mechanisms of international legal cooperation in the field of prosecution.

The anonymity or pseudonymity of DAO participants, which is a technically determined property of blockchain systems, significantly complicates the application of classical institutions of civil, administrative, and criminal liability. In particular, it is impossible to properly identify the defendant, prove a causal relationship between the actions of a particular person and the damage caused, as well as enforce court decisions. As a result, there is a risk of actual irresponsibility of decentralised entities, which contradicts the fundamental principles of law and order and the principle of inevitability of legal responsibility.

In modern scientific doctrine, the position according to which the cross-border activities of decentralised autonomous organisations cannot be effectively regulated exclusively with the help of general rules of private international law are being substantiated more and more consistently. The specificity of DAOs as decentralised digital entities that operate without a clear territorial reference necessitates the formation of special conflict rules aimed at determining the applicable law, competent court, and procedures for bringing to legal responsibility.

In this context, the issue of legal identification of DAO participants who exert a significant or decisive influence on the organisation's activities acquires special importance. The doctrine proposes the introduction of mandatory identification mechanisms for such persons, in particular in cases where the activities of the DAO are of a publicly significant nature, are related to the management of significant financial resources, or create increased risks to the rights and legitimate interests of third parties.

The introduction of special conflict of laws regulation in combination with differentiated requirements for the identification of key DAO participants would ensure a balance between the principle of technological decentralisation and the fundamental requirements of legal certainty, predictability of law enforcement and effective judicial protection. Such an approach would correspond to the general trend in the development of digital law, aimed at adapting classical legal institutions to new forms of socio-economic interaction in the global digital environment.

2.3.4. Regulation of DAOs in the United States.

The United States of America is one of the few jurisdictions in which consistent and practically oriented steps have been taken towards the normative recognition of decentralised autonomous organisations. The most developed and conceptually complete in the legal sense is the approach of the state of Wyoming, which introduced a special legal form DAO LLC as a type of limited liability company. The relevant legislative changes provide for the possibility of registering a DAO, subject to the disclosure of basic information about governance mechanisms, smart contracts, and the nature of decentralised decision-making.

The introduction of the DAO LLC model is of significant legal importance from the standpoint of the theory of corporate and business law, as it allows granting a decentralised autonomous organisation limited legal personality within the legal order of a particular state. Such legal personality, although derivative in nature, provides for the possibility of legal participation of the DAO in civil turnover, in particular the opening of

bank accounts, the acquisition and alienation of property, the conclusion of civil and commercial contracts, as well as acting as a party in judicial and administrative procedures.

A key element of this model is the legally enshrined limitation of liability of DAO participants, which functionally brings their legal status closer to the participants of classic limited liability companies. Members of DAO LLC, as a general rule, are not personally liable for the obligations of the organisation, unless otherwise expressly provided by law or arising from proven facts of abuse of rights, fraud or wilful violation of fiduciary duties. This approach significantly reduces legal risks for DAO participants and contributes to attracting investments, while providing a basic level of protection for the rights of creditors and third parties.

From a legal point of view, the DAO LLC model can be considered as an institutional compromise between the principle of decentralised autonomy and the classical principles of corporate law, in particular the principles of legal certainty, limited liability and predictability of the legal status of participants in organisational entities.

In addition, the incorporation of a DAO into the form of an LLC is essential from the standpoint of financial and tax law, as it ensures the integration of such entities into the tax system of the United States of America and the application of general rules of tax accounting and reporting to them. Registering a DAO in the form of an LLC allows them to apply clear and predictable tax regimes, in particular the principle of "pass-through taxation", according to which tax liabilities arise directly from the participants, and not at the level of the organisation, unless otherwise chosen in accordance with tax legislation. This significantly reduces the level of regulatory uncertainty and contributes to the legalisation of financial flows related to DAO activities.

At the same time, Wyoming legislation does not aim to fully institutionalise or "centralise" decentralised autonomous organisations. On the contrary, it preserves the algorithmic nature of management and the autonomy of the DAO's internal processes, limiting itself to the creation of a so-called "legal wrapper". Such a shell performs the function of an external legal framework that combines decentralised algorithmic management with standard requirements of corporate, financial and tax law, in particular regarding transparency, accountability and protection of the rights of third parties.

In the legal doctrine, this approach is considered as a pragmatic compromise between the principles of technological decentralisation and the need to ensure legal certainty, predictability of the legal status of participants and effective protection of the rights of creditors and other interested parties. At the same time, The lack of a unified federal approach preserves the fragmentation of regulation and creates legal asymmetry between states.

2.3.5. Regulation of DAOs in the European Union.

In the law of the European Union, decentralised autonomous organisations are currently not recognised as independent subjects of law and do not have a separately defined organisational and legal status. Regulation of DAOs is carried out in fragments and indirectly through the application of EU secondary law acts aimed at regulating certain aspects of the digital economy, financial markets and protection of fundamental rights.

First of all, we are talking about the Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), which establishes comprehensive requirements for issuers of crypto-assets, crypto-asset service providers (CASPs), as well as consumer protection and financial stability mechanisms. While MiCA does not explicitly regulate DAOs as organisational entities, its provisions actually apply to a significant portion of DAO activities, particularly in cases of token issuance, crypto asset management, or the provision of decentralised financial services.

The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) also plays an important role, which applies to the processing of personal data within the DAO, regardless of its decentralised nature. This raises complex legal issues regarding the definition of the controller and processor of data in decentralised systems, the distribution of responsibilities among DAO participants, and the implementation of the rights of personal data subjects in an environment of immutable distributed ledgers.

In addition, the activities of individual DAOs may be subject to the provisions of Regulation (EU) 2022/858 on the pilot regime for market infrastructures based on distributed ledger technology (DLT Pilot Regime), Regulation (EU) 2022/2554 on the digital operational resilience of the financial sector (DORA), as well as Directive (EU) 2022/2555 (NIS2), which establishes increased requirements for the cybersecurity of critical digital actors.

In general, the European approach to DAOs is characterised by regulatory caution, the priority of consumer protection, financial stability, and fundamental rights, as well as the desire to adapt existing legal instruments to new technological models without introducing a separate legal form for DAOs. Such an approach, on the one hand, minimises regulatory risks, and on the other hand, it preserves legal uncertainty regarding the status, responsibility and internal governance of decentralised autonomous organisations in the legal order of the European Union.

At the same time, scientific, expert and advisory circles of the European Union are actively discussing the feasibility of introducing a special legal regime for decentralised autonomous organisations, in particular through the model of the so-called "legal wrapper". Within the framework of this approach, it is proposed not to create a new organisational and legal form at the level of EU primary law, but to adapt the existing constructions of corporate, financial and digital law by granting DAOs limited and functionally determined legal personality. The discussion of this model is taking into account the provisions of Regulation (EU) 2023/1114 (MiCA), Regulation (EU) 2016/679 (GDPR), Regulation (EU) 2022/858 (DLT Pilot Regime), as well as EU digital governance acts, in particular Regulation (EU) 2022/2065 (Digital Services Act) and Regulation (EU) 2022/1925 (Digital Markets Act). The introduction of a "legal shell" for DAOs is seen as a potential mechanism to eliminate legal uncertainty regarding the responsibility, governance and accountability of decentralised entities without violating the basic principles of technological neutrality and subsidiarity of European Union law.

2.3.6. DAO as a tool for algorithmic compliance.

DAOs can potentially perform the function of algorithmic compliance as a special legal mechanism for ensuring compliance with regulatory and regulatory requirements in the digital environment. Within this model, the prescriptions of law are implemented directly into the program code of smart contracts, which function as technical and legal tools for the implementation of legal norms. Accordingly, legal requirements are transformed into algorithmic rules of conduct that are applied automatically and equally to all DAO participants, without the possibility of selective or discretionary application.

Compliance with such rules is ensured not by traditional forms of post-factum control, administrative supervision or authorisation, but through automated and inevitable fulfilment of the conditions laid down in smart contracts. From a legal point of view, this means a shift in emphasis from repressive enforcement mechanisms to preventive ones, when violation of regulatory requirements becomes technically impossible or economically unprofitable. This approach allows you to significantly minimise the discretionary factor in the process of implementing legal norms, reduce the risks of human error, and limit the possibilities of abuse of rights by individual DAO participants.

At the same time, algorithmic compliance cannot be considered as a complete replacement for traditional legal mechanisms. The formalisation of legal prescriptions in the form of program code is inevitably associated with the risks of incompleteness or simplification of the normative content, especially in cases where the law operates with evaluative categories, the principles of proportionality, reasonableness or justice. This necessitates the normative definition of the limits of the application of algorithmic compliance, as well as the establishment of clear rules of legal responsibility for errors in the design of smart contracts or defects in the algorithmic implementation of legal requirements.

From a legal point of view, algorithmic compliance within a DAO can be considered as a form of preventive law enforcement in which regulatory violations become technically impossible or economically impractical. At the same time, such a model does not eliminate the need for external legal control, since smart contracts only implement predetermined rules and are not able to independently take into account the evaluative categories of law, the principle of proportionality or the public interest.

This approach conceptually correlates with the Zero Trust Architecture (ZTA), which was initially formed in the field of cybersecurity and information systems management, but gradually acquired interdisciplinary importance, in particular in the field of legal regulation of digital organisations. The fundamental principle of the Zero Trust Architecture is to abandon a priori trust in any entity or component of the system, regardless of its internal or external status, and replace it with a model of permanent, contextual and dynamic verification of each action, transaction or access request.

In the legal dimension, the application of the Zero Trust Architecture principles to the activities of DAOs means the transformation of traditional ideas about trust as a socio-legal category. If in classical organisational and legal forms, trust is based on the personal responsibility of governing bodies, corporate control or state supervision, then in the case of DAOs it is replaced by trust in the protocol as a set of formalised, verifiable and technically supported rules. The protocol in such a model performs the function of a

technical and legal guarantor of compliance with the established norms, ensuring the equal application of the rules to all participants without discretion and selectivity.

From the standpoint of the theory of law, the Zero Trust Architecture can be considered as the basis for the formation of a new type of regulatory logic, within which control and responsibility are implemented not only through institutional mechanisms, but also through the architecture of the system. Each action of a DAO participant is subject to a preliminary check for compliance with algorithmically fixed legal requirements, which brings the governance model closer to the continuous compliance regime. At the same time, such a model does not eliminate the need for a legal assessment of the consequences of actions, especially in cases of system failures, code errors or incorrect formalisation of legal norms.

Therefore, the implementation of the Zero Trust Architecture principles in the activities of DAOs is essential for the development of modern approaches to the regulation of digital organisations, but objectively requires a clear regulatory definition of the boundaries of algorithmic regulation, external oversight procedures and mechanisms of legal responsibility for defects in program code or errors in the translation of legal prescriptions into algorithmic form.

2.3.7. Five-Tier DAO Architecture for the Metaverse.

Let's summarise a typical multi-layer DAO architecture as the basis of five-level platform governance**:**

a) Infrastructure: blockchain, network protocols, nodes, data warehouses (on-chain/off-chain), identity mechanisms.

It is advisable to consider the infrastructure level of the DAO as an operational, technological, and legal element of the digital state, which ensures the implementation of the principles of decentralisation, subsidiarity and functional autonomy within public administration. In this context, the DAO acts not as a tool of local governance, but as a basic infrastructure layer of digital statehood, capable of providing distributed decision-making, automated implementation of rules, and increased transparency of government processes without concentrating control in a single administrative centre.

The use of public or consortium blockchain networks within DAOs creates technical prerequisites for the formation of a distributed system of public administration, where power and administrative functions are implemented through protocols, smart contracts, and formalised access rules. The absence of a single centre of control does not mean the absence of statehood as such, but, on the contrary, transforms it into a network form in which legitimacy and accountability are ensured by the architecture of the system, and not by the hierarchy of institutions.

The placement of nodes in such a model can be carried out by various public infrastructure entities or accredited operators of the digital state, which allows to ensure the stability, fault tolerance and institutional neutrality of the system. Such an architecture reduces the dependence of the digital state on separate centralised platforms — both public and private — and at the same time creates conditions for interoperability between different segments of public digital services.

On-chain and off-chain data warehouses within DAOs perform not only a technical but also a regulatory function. Data of legal, financial or regulatory significance (results

of electronic voting, algorithms for the distribution of public resources, rules for the provision of digital services, terms of government programs) can be recorded unchanged in a distributed register. At the same time, personal data, proprietary information of limited access, or information subject to special protection regimes is processed outside the blockchain in compliance with the requirements of the legislation on personal data protection and information security.

Such a dual approach to the storage and processing of information allows you to combine the principle of public transparency with the principle of legitimate limited access and respect for privacy. In the legal dimension, this forms a new model of public accounting and control, where the immutability and provability of data are achieved by technical means, and not exclusively through administrative procedures or trust in officials.

Of particular importance in the architecture of the digital state are decentralised digital identity mechanisms integrated with DAOs. They provide proof of a person's legal personality or digital agent status without creating single, centralised ledgers that are traditionally vulnerable to abuse, data leaks, or political influence. The application of Zero Trust Architecture approaches assumes that every transaction or managerial action is subject to verifiability, but is not based on the presumption of unconditional institutional trust.

Summing up, the infrastructure layer of DAOs in the digital state model forms the technical and legal prerequisites for the transition from hierarchical to protocol statehood, where management is carried out through formalised algorithms, verifiable rules, and distributed responsibility. It is this architecture that can ensure the long-term sustainability of the digital state, its adaptability to technological changes and increasing the level of legal certainty in digital public administration (Figure 32).

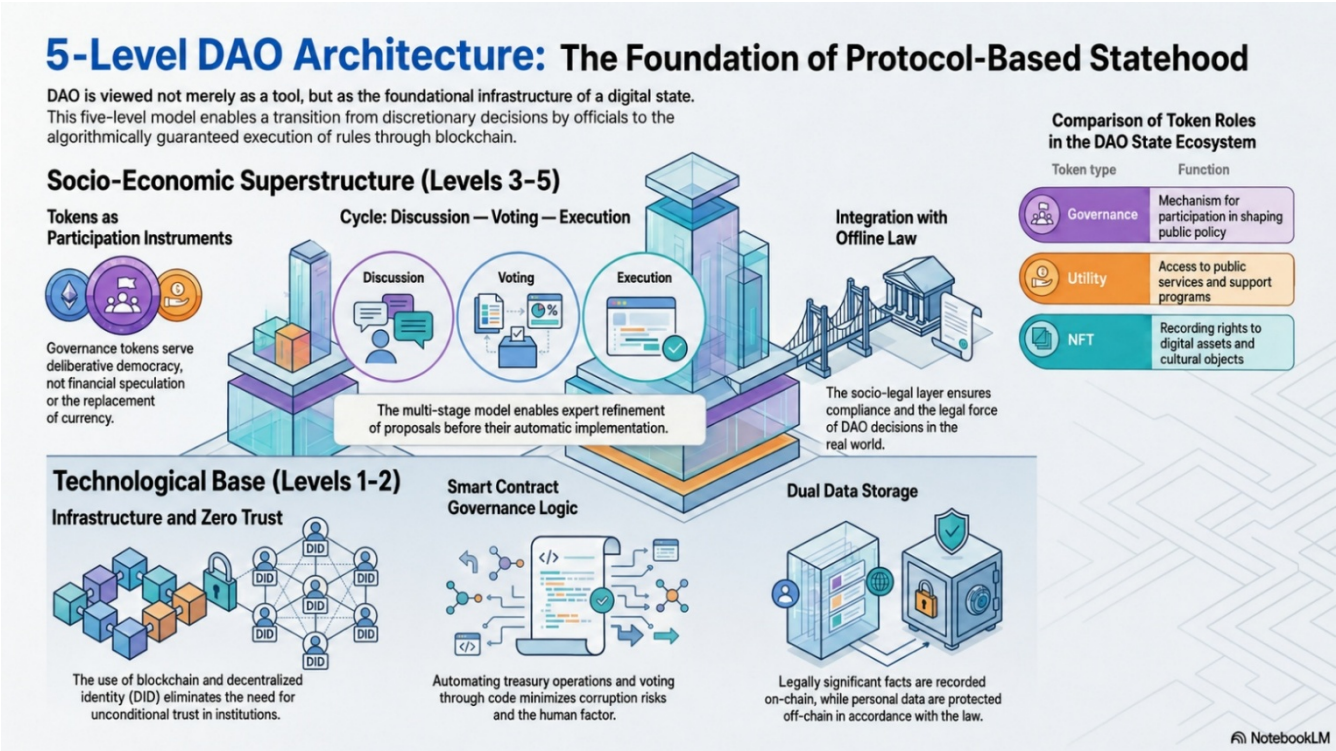


Figure 32. Metaverse: DAO Five-Tier Architecture.

b) Smart contract logic: voting rules, treasury, grant programs, asset markets.

Smart contract logic is central to the functional architecture of DAOs and acts as a key operational layer of the digital state, where the principles of decentralisation, participation, automated accountability, and procedural certainty are practically implemented. It is through smart contracts that the rules for collective decision-making, public finance management, and administration of programs for the development and circulation of digital assets are formalised in the form of algorithmically set and legally relevant norms of behaviour.

The voting rules enshrined in smart contracts ensure transparent, open and verified expression of the will of digital statehood entities within various forms of electronic participation. In the legal dimension, such mechanisms can be used for consultative surveys, e-consultations, strategic votes or other collective decision-making procedures in the public sector. Algorithmic fixation of voting procedures makes it impossible to manipulate the results, selectively interpret the rules or change them in the process of application, which directly corresponds to the principles of legal certainty, equality of participants and predictability of state decisions.

The DAO treasury, implemented on the basis of smart contract logic, can serve as a decentralised mechanism for managing the public financial resources of the digital state. We are talking about the automated administration of budget programs, trust funds, innovation or infrastructure projects, where smart contracts ensure the unconditional implementation of the approved funding rules. This model provides for the targeted use of funds, transparent recording of all transactions and the impossibility of unauthorised interference in financial flows.

c) Tokens and economy: governance tokens, utility tokens, NFT assets (land, items, rights).

The token-economic layer of the DAO plays a systemic role in shaping decentralised models of participation, incentives, and resource allocation within the digital state. In this architecture, tokens appear not only as economic units, but as multifunctional legal and social tools, with the help of which models of participation of subjects in public processes are structured, rights and obligations are fixed, and motivation for collective action in the digital public environment is provided.

Governance tokens within a digital state can be used as a formalised mechanism for individuals to participate in the processes of developing, adjusting, and evaluating public policies. In the legal dimension, such tokens are not holders of sovereign powers and do not replace constitutional institutions of representation, but they are able to ensure the implementation of advisory, consultative and procedural-participatory forms of digital democracy. Algorithmic consolidation of voting rights through governance tokens contributes to transparency and reproducibility of procedures, while at the same time requiring regulatory restrictions on the concentration of influence, prevention of access asymmetry, and risks of "tokenised oligarchisation" of decision-making processes.

Utility tokens in the architecture of a digital state can perform the functions of accessing digital public services, participating in support programs, using infrastructure or cultural resources, as well as stimulating socially useful and innovative activity. From a legal point of view, it is advisable to consider such tokens not as financial instruments in the classical sense, but as elements of the internal public-digital economy that function

within the framework of specially defined government programs. Their legal regime should be clearly distinguished from means of payment and financial derivatives in order to avoid conflict with budgetary, financial and monetary law.

NFT assets (non-fungible tokens) in the digital state open up opportunities for representation, accounting, and verification of rights to digital or tokenised objects of public importance. These include, in particular, digital infrastructure facilities, cultural or historical artifacts in virtual form, as well as the right to access, use, or participate in joint state or socially significant projects. In the legal dimension, NFTs do not replace traditional proprietary or obligatory rights, but they can perform an evidentiary, accounting, or representative function, provided that their legal nature and relationship with offline law are clearly defined.

It is important to emphasise that the DAO token economy within the digital state should not be focused on financial speculation, but on the institutionalisation of participation, the stimulation of responsible behaviour, and the efficient allocation of public resources. In this sense, tokens act as instruments of public policy rather than objects of private investment, which requires a fundamentally different approach to their legal regulation and control.

Overall, the token-economic layer of the DAO forms a regulatory-sensitive digital statehood infrastructure in which economic incentives, participation in governance, and legal attribution interact in a single protocol system. The effectiveness of this model is possible only if special legal safeguards are introduced, in particular, a ban on the use of tokens as surrogates for money, a clear distinction between public and private economic interests, and the alignment of token models with the principles of legal certainty, democratic legitimacy, and functional decentralisation of the digital state.

e) Governance: proposal procedures, delegation, quorums, multi-stage (discussion → voting → implementation).

The management level of the DAO is central to the structure of the digital state in terms of implementing decentralisation as a legal, organisational and institutional principle. It is at this level that the protocol architecture of collective expression of will is formed, which ensures the participation of digital statehood entities in the development of managerial decisions, their legitimation, procedural accountability and formal reproducibility. In this dimension, the DAO acts not as a tool of local governance, but as a universal model of distributed public administration, integrated into the general system of digital statehood.

The procedures for submitting proposals enshrined in smart contracts serve as an institutionalised channel for the initiative within the digital state. They form a formalised mechanism for introducing managerial, regulatory or program initiatives into the decision-making system. In the legal dimension, this corresponds to the concept of procedural participation of subjects in public administration, where the right of initiative acquires not a political, but an algorithmic-legal form. Algorithmic determination of requirements for proposals — support thresholds, review periods, eligibility criteria — ensures equality of access to management procedures and minimises the risks of selective, discretionary or biased consideration of initiatives.

Delegation mechanisms in DAOs create a model of combining direct and representative democracy within digital statehood. Entities may delegate their managerial

authority or votes to other participants, expert agents, or digital representatives, while retaining the right to revoke the delegation. In the legal sense, such a construction forms a new model of representation based not on fixed hierarchies, but on dynamic, revocable and protocolally fixed relations of representation, which corresponds to the principles of accountability, openness and functional flexibility.

Quorums and vote counting rules in DAOs play a fundamental role in ensuring the legitimacy of governance decisions. Algorithmic fixation of minimum participation thresholds, qualified majorities, and special voting modes prevents decision-making by narrow active groups without sufficient public support. In the legal dimension, this forms procedural guarantees of representativeness, legal certainty and prevention of concentration of managerial influence within distributed systems.

The multi-stage governance model (discussion → voting → execution) embedded in the DAO architecture provides a logical, procedural, and legal consistency of decision-making. The stage of public discussion creates a space for rationalisation of positions and expert correction of proposals, the stage of voting — for the formalisation of collective will, and the stage of automated implementation — to eliminate the risks of selective, untimely or politically motivated implementation of decisions. In a legal sense, this meets the standards of good governance, procedural fairness and administrative predictability.

The institutional feature of the DAO approach is that governance is transformed from a hierarchical-administrative model into a protocol-normative one, where the source of legitimacy is not the authority as such, but a formalised procedure enshrined in the code and normatively verified by law. Thus, law, algorithm and procedure merge into a single system of management regulation.

In general, the management level of the DAO forms the legal and operational architecture of the digital state, in which decentralisation appears not as a political slogan, but as a technologically implemented legal mechanism. — In my opinion, it is this level that is the core of the transition to protocol statehood, where the legitimacy of power is based on formalised procedures, algorithmic verifiability of decisions and legally defined models of participation, provided that the boundaries of the use of such instruments and their integration into the public law system are clearly fixed.

g) Social and legal level: participants, reputation, moderation, legal status, integration with offline law, compliance.

The socio-legal level of the DAO is the final and at the same time the backbone element of the five-layer architecture, since it is at this level that the integration of technological mechanisms of decentralised governance with social relations, legal norms, and the institutional environment of the digital state takes place. This level determines how DAO entities acquire and implement their legal status, how trust and responsibility are formed in the digital community, as well as how the DAO's activities are aligned with the requirements of offline law and public order.

DAO participants within digital statehood can perform various functional roles: users of public digital services, experts, project initiators or executors, auditors, observers, or digital agents with a limited mandate. From a legal point of view, it is fundamentally important to clearly distinguish such roles and determine the scope of rights, duties and responsibilities of each category of participants. This avoids mixing advisory, executive and control functions and ensures that the functioning of the DAO complies with the basic

principles of public law, in particular the principles of legality, proportionality and legal certainty.

Reputation mechanisms in DAOs can serve as a non-monetary tool of social and legal regulation in a digital state. Reputation formed on the basis of recorded participation in the processes of discussion, voting, implementation of decisions or implementation of publicly significant projects can affect the level of trust in the participant and the permissible limits of his participation in further management processes. In the legal dimension, reputational systems should not replace legal liability or judicial protection, but they can complement formal legal mechanisms, contributing to self-regulation and improving the quality of collective management.

Moderation in DAOs, especially in processes of public law importance, should be carried out on the basis of transparency, procedural fairness and accountability. Algorithmic moderation or hybrid models combining automated and human mechanisms can be applied to prevent abuse, manipulation or violation of established rules. At the same time, such tools need a clear regulatory definition, in particular regarding the grounds and limits of interference, procedures for appealing decisions, and guarantees of protection of the rights and freedoms of participants in digital interaction.

The socio-legal level is of particular importance for determining the legal status of DAOs and the legal force of the results of their activities in the plane of offline law. Decisions made within the framework of the DAO may be advisory, advisory, analytical or preparatory in nature for public authorities, but cannot automatically generate legally binding consequences without proper legal formalisation in the forms and procedures provided for by law. This approach ensures the consistency of decentralised digital mechanisms with the principle of the rule of law and prevents the substitution of algorithmic solutions for legal procedures.

The integration of a DAO with offline law also involves compliance in key areas of public administration, including personal data protection, information security, financial discipline, anti-corruption standards, and public accountability. In this context, DAOs can act not only as an object of legal regulation, but also as a tool for its strengthening, ensuring transparency of procedures, traceability of actions, and fixation of management decisions in an unchanging digital environment.

An important aspect of the social and legal level is also the formation of trust in the digital state as such. Trust in this model does not arise from the authority of the institution, but from a combination of technical verifiability, procedural fairness and normative certainty. A DAO, in this sense, serves as an environment in which law, social interaction, and technology form a single system of mutual reinforcement.

As a result, the socio-legal level of DAOs forms a bridge between decentralised technologies and the legal reality of the digital state, ensuring their institutional compatibility and legitimacy, which is crucial for the transition from experimental DAO models to their full integration into the public law system, since without a clear socio-legal framework, even the most advanced technological solutions remain normatively vulnerable and socially unstable.

2.3.8. Functionality of DAOs in public administration of Ukraine.

In the context of digital transformation of public administration, decentralised autonomous organisations (DAOs) should be considered as an auxiliary, institutionally neutral tool for increasing transparency, accountability, and procedural openness in the processes of forming and implementing public policy. It is not about the transformation or replacement of public authorities or holders of sovereign powers, but about the use of DAOs as a technical and organisational mechanism for supporting decision-making, digital support of management processes and improving the quality of interaction between the state and citizens within the limits determined by law.

In this context, DAOs can perform the function of a procedural infrastructure of a digital state, providing formalisation of consulting, analytical, and monitoring processes. Their institutional neutrality lies in the fact that they are not endowed with their own power competence, but act as an environment for the implementation of predetermined legal procedures. This approach allows using the technological advantages of decentralised systems without violating the principle of unity of public power and the constitutional model of statehood.

Potential areas of application of DAOs in the public administration system include, among others, e-democracy tools such as consultative voting, e-petitions, public discussions, and strategic surveys. DAO algorithmic mechanisms in these processes are able to ensure the transparency of procedures, immutability of results, verification of vote counting, and reproducibility of management decisions. In the legal dimension, this reinforces guarantees of procedural fairness and trust in the results of citizens' participation in public processes.

In the field of citizen participation in the allocation of public resources, DAOs can be applied for the automated administration of participation programs, including the allocation of funds in accordance with pre-approved rules. Smart contract logic allows minimising the risks of selective interference, manipulation or corruption abuse, since the execution of financial decisions takes place within the framework of formalised algorithms open to verification and audit.

Special attention should be paid to the possibility of using DAOs to manage public funds, grant programs, and recovery and development projects. In such models, smart contracts can perform the function of financial control tools, ensuring the intended use of funds, and continuous reporting. Algorithmic oversight of the fulfilment of funding conditions brings public resource management closer to the standards of continuous compliance and the Zero Trust architecture, where every action is subject to verification without the presumption of unconditional trust.

At the same time, the integration of DAOs into public administration is possible only if the priority of constitutional principles is maintained, the demarcation of advisory and power functions is clearly distinguished, and there are normatively defined mechanisms of legal responsibility. DAOs cannot be considered as autonomous subjects of public power or alternative centres of binding decision-making, as this would contradict the principle of the rule of law and the democratic legitimation of state power.

From a legal point of view, DAOs should be perceived as digital governance tools, subject to the public law regime, administrative procedures, and democratic control. Their application requires a clear normative consolidation of the boundaries of functioning, the

legal status of the results of activities and procedures for integration with offline decision-making mechanisms. Only under such conditions can DAOs strengthen, not replace, the institutional capacity of the state.

To summarise, DAOs in the digital state system act as a technological catalyst for transparency and accountability, but not as sources of public power. — In my opinion, their strategic value lies precisely in their instrumentality: DAOs allow the state to move from declarative openness to procedurally guaranteed transparency, without destroying the constitutional foundations of public administration and legal order.

2.3.9. Constitutional and Legislative Limitations of DAOs.

The use of decentralised autonomous organisations in the system of public administration of Ukraine is objectively limited by the basic principles of the constitutional order, primarily the principles of popular sovereignty, the rule of law and the separation of powers. The constitutional model of statehood is based on the fact that the bearer of sovereignty and the only source of public power is the people, who exercise it directly or through institutions determined by the Constitution and laws. Under such conditions, any transfer of power and management functions to algorithmic or automated systems without a clear legislative mandate would contradict the fundamental provisions of constitutional law.

The issue of the admissibility of automated management decision-making in the public law sphere requires special attention. The current legislation of Ukraine is based on the presumption of personal or collegial responsibility of public authorities for the results of the implementation of public competence. In the administrative-legal and constitutional-legal dimensions, responsibility is inextricably linked to a specific official or body endowed with the relevant mandate. Algorithmic systems, including DAOs, cannot bear such responsibility, which makes it impossible to consider them as subjects of the will of power.

From a legal point of view, this means that DAOs are not able to act as addressees of public law norms that provide for legal liability for illegal, erroneous or unfair management decisions. The absence of the possibility of bringing the algorithmic system to justice would violate the principles of legal certainty, effective protection of human rights and freedoms, as well as the principle of accountability of public authorities, which is the cornerstone of a democratic state governed by the rule of law.

An additional limiting factor is the absence of legal personality of DAOs as legal entities or as special public law entities in the current legislation of Ukraine. Neither civil, administrative, nor financial legislation provides for the existence of DAOs as independent subjects of law capable of acquiring rights and obligations in public law relations. This excludes the possibility of their use as independent holders of powers, managers of public resources or parties in power-administrative legal relations.

In the absence of regulatory recognition, DAOs can function in the field of public administration exclusively as auxiliary technical and organisational tools. In this case, their activities should be clearly subordinated to public authorities, carried out within the framework of delegated procedural functions and be under constant legal and institutional control. DAOs in this model do not replace government entities, but only provide

technological support for the implementation of management decisions that have already been made.

Constitutional and legislative restrictions also necessitate a clear distinction between advisory, analytical and power functions. Any results obtained with the help of the DAO can only be of an auxiliary, advisory or information-analytical nature and require further legal formalisation in the forms and procedures determined by law. This ensures the consistency of digital tools with the rule of law and prevents the substitution of algorithmic solutions for legal mechanisms.

As a result, constitutional and legislative restrictions establish clear limits on the use of DAOs in the public sector of Ukraine, excluding the possibility of their functioning as autonomous centres of public power. —In my opinion, these restrictions should be considered not as a barrier to digitalisation, but as a legal framework that allows the integration of DAOs into the public administration system without violating constitutional legitimacy, democratic accountability, and the rule of law (Figure 33).



Figure 33. Metaverse: DAO in public administration of Ukraine.

2.3.10. Prospects for regulatory consolidation of DAOs.

In Ukraine, it is expedient to form a special, comprehensive legal regime of decentralised autonomous organisations, which would take into account their technical and organisational specifics and at the same time meet the requirements of the national constitutional legal order. Such a regime should not be based on the full institutionalisation of the DAO as a new form of legal entity, but on the creation of a normatively defined "legal framework" within which DAOs could function as special digital organisational entities of a private or mixed nature, integrated into the ecosystem of the digital state.

Conceptually, this legal regime should proceed from an instrumental approach to DAOs, considering them not as independent carriers of public power, but as technological structures capable of providing support for managerial, analytical and procedural

processes. This approach allows you to preserve the integrity of the constitutional model of statehood, without denying the possibilities of using decentralised technologies to increase the efficiency, transparency and accountability of public administration.

It is expedient to determine the key elements of the special legal regime:

Firstly, a mechanism for voluntary state registration of DAOs, which would provide a minimum level of legal identification of the organisation without destroying the principle of decentralisation and autonomy. Such registration should not turn the DAO into a classic legal entity, but should create a legal "anchor" necessary for interaction with state institutions, financial systems, and public control mechanisms.

Secondly, an important element is the mandatory or conditionally mandatory audit of DAO smart contracts, aimed at verifying their compliance with the requirements of the law, the principles of non-discrimination, information security and human rights protection. Such an audit should identify hidden or harmful algorithmic mechanisms, ensure transparency of governance rules, and minimise the risks of abuse, which is especially important in cases where DAOs are used in publicly significant processes.

Thirdly, legal regulation should provide for the normative consolidation of mechanisms for identifying participants who have a significant or decisive influence on the activities of DAOs. It is not about the complete de-anonymisation of all participants, but about a differentiated approach, in which increased identification requirements are applied depending on the nature of the DAO's activities, the scale of resource circulation, and the degree of impact on public interests.

A separate legal regulation requires the use of DAOs in the digital public administration system as such. In this context, the regulatory goal should not be to severely restrict or ban DAOs, but to create conditions for their use as tools to increase citizen participation in public processes, increase the transparency of government programs and improve public resource management procedures. DAOs can act as an environment for electronic consultations, analytical support for decisions, monitoring program execution, and automated administration of individual procedures.

At the same time, the imperative limitations of such a legal regime should clearly record the inadmissibility of delegating to the DAO the authority itself related to the adoption of legally binding management decisions, the exercise of discretionary functions or the implementation of coercion on behalf of the state. DAOs in this model can function exclusively as auxiliary technical and organisational mechanisms, the results of which acquire legal significance only after they are formalised by authorised public authorities.

The proposed approach is consistent with the constitutional principles of public administration and the principle of the rule of law, as it provides a clear distinction between the sphere of algorithmic support and the sphere of the expression of power. The activities of DAOs in publicly significant processes should be carried out under the normatively defined control of the state and accompanied by the clearly established legal responsibility of officials and participants involved in the integration of such technologies.

As a result, the introduction of a special legal regime for DAOs would combine the innovative potential of decentralised technologies with the requirements of legal certainty, predictability of the legal status of participants, and constitutional legitimacy of public authorities. — In my opinion, it is such a framework model that can become the basis for the further development of national legislation in the field of digital governance, algorithmic systems and the formation of an integral architecture of the digital state.

2.4. Digital twins in the Metaverse: legal regime and features of use

2.4.1. Digital Twins.

In the context of information law, it is advisable to consider a digital twin (DT) not only as a technological tool, but as a complex information and legal object that acts as an infrastructural element of the Metaverse and mediates legally significant information processes. Its key function is to ensure a continuous, formalised and legally relevant information connection between the physical object, the social activity of the subjects and their digital representation in the virtual environment. Unlike traditional virtual models, the digital twin is not limited to reproducing the external characteristics of the object, but functions as a dynamic information and algorithmic system capable of accumulating, processing, correlating and transmitting data from physical sensors, information systems and social platforms in a mode close to real time.

Let's apply the author's definition: A digital twin as an element of the Metaverse is a legally relevant informational and algorithmic model of a physical, social or procedural object or a structured array of organised data and algorithms and an infrastructural component of a cyber-physical and social system that combines physical reality, social activity and a virtual environment, which operates in the mode of continuous data updating and is capable of generating legal consequences in the digital environment by fixing, processing and broadcasting information, as well as provides a formalised reflection of the state and behaviour of the object and acts as an object of legal regulation regarding access, control, responsibility and data protection.

From an information and legal point of view, the Metaverse digital twin should be qualified as a special form of organised data that has the characteristics of a digital asset and a potential object of legal regulation. Such a system generates and uses data sets, which may include personal data, industrial data, technical telemetry and algorithmic processing results, which actualises the issues of the legal regime of access, ownership, control and responsibility for their use. Accordingly, the digital twin in the Metaverse forms not only a technological, but also a normative reality, within which information legal relations arise between owners of physical objects, operators of digital platforms, algorithm developers, and end users.

In modern Metaverse architectures, digital twins are increasingly being formed using graph neural networks and other machine learning models, which have not only technical, but also direct informational and legal significance. The use of such models makes it possible to formalise complex nonlinear relationships between elements of cyber-physical and social systems, turning them into structured data sets suitable for legally significant processing, analysis, and use in regulatory and evidence-based goals (Ma et al., 2023)[1].

Metaverse digital twin models are built and evolved in parallel with their respective physical objects or processes, providing the ability to predict, simulate, and optimise the behaviour of systems without directly interfering with material reality. From the information and legal point of view, this means the emergence of a new form of

1Ma, W., Liu, M., Hong, G., Yang, S., & Deng, R. (2023). Grid-metaverse: The path from digital twins and prototype tests on DC microgrids. *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, 290–296. https://doi.org/10.1109/MetaCom57706.2023.00059

algorithmically mediated influence on the objects of management, which requires a clear definition of the boundaries of permissible use, the legitimacy of decision-making and the distribution of legal responsibility between the entities that create, administer and operate digital twins.

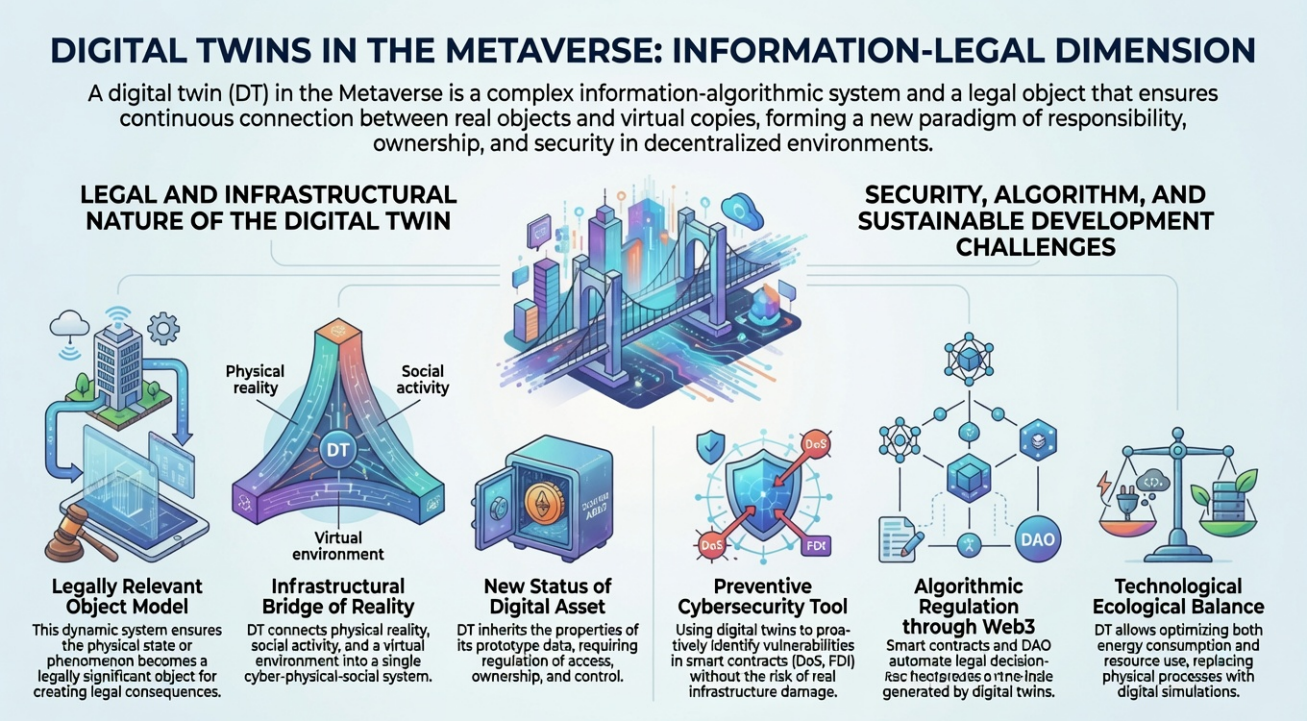


Figure 34. Metaverse: digital twins.

In the context of the Grid-Metaverse, digital twins act as nodal elements of a distributed information infrastructure, combining computing resources, data, and digital environments into a single integrated ecosystem. This role determines their consideration as critical information objects, the functioning of which directly affects the integrity, reliability, and legal significance of data in the Metaverse (Figure 34). Accordingly, digital twins acquire the characteristics of elements of the information infrastructure of increased legal responsibility, which actualises the issues of their regulatory protection, certification and inclusion in information security regimes.

The use of digital twins for modelling, identification, and legal assessment of information security threats, in particular denial-of-service (DoS) attacks and False Data Injection (FDI), acquires a separate, independent significance in the information and legal dimension. In such cases, digital twins perform the function of a specialised tool for preventive analysis, which allows you to reproduce scenarios of cyber incidents, assess their potential consequences and determine the degree of damage to information resources without actually interfering with the functioning of real critical infrastructure facilities.

From the point of view of information law, this creates fundamentally new opportunities for the formation of an evidence base, an audit of information security and the fulfilment of obligations for proper data protection assigned to owners and operators of information systems. The use of DT for testing and verification of protective mechanisms allows you to record technical and organisational shortcomings of the system

in advance, which is of direct importance for determining legal liability in the event of damage. Thus, digital twins are an element of the information security infrastructure, which combines technical means of protection with legal mechanisms of prevention, compliance and distribution of responsibility between the subjects of information legal relations.

2.4.2. Metaverse as a Cyber Physical-Social Paradigm Digital Twins.

The convergence of Web3, Metaverse, and Digital Twins technologies forms a qualitatively new cyber-physical and social paradigm that has direct information and legal consequences for the regulation of social relations in the digital environment. Within this paradigm, digital, physical and social processes are integrated into a single information environment in which data, algorithms and digital representations of objects acquire legal significance. Web3, built on blockchain architecture and decentralisation principles, creates technological prerequisites for the implementation of information rights of subjects, in particular the right to control their own data, digital assets, and identification attributes, which actualises the issue of the legal regime of ownership, disposal, and responsibility in decentralised systems.

The Metaverse, in turn, forms an immersive digital space as a special information and legal environment, within which economic, professional and cultural practices are carried out, giving rise to new types of information legal relations. In such an environment, the interaction of subjects takes place not only on a contractual basis, but also through algorithmically determined platform rules, which necessitates a rethinking of classical approaches to jurisdiction, responsibility and protection of participants' rights. Thus, the convergence of Web3, Metaverse, and digital twins lays the foundation for the formation of a new model of information law and order, in which the technological architecture directly affects the content and way of implementing legal norms.

Digital twins within the specified triune system perform the function of not only a technological, but also an informational and legal "bridge" between the physical world, the social activity of subjects and the virtual environment of the Metaverse. They provide a formalised binding of data within the Cyber-Physical-Social Systems (CPSS), as a result of which physical processes, social interactions and behavioural patterns acquire the status of legally relevant digital mappings suitable for use in legal regulation, control and evidence.

From an informational and legal point of view, such data binding means the continuity and reproducibility of information processes in cyberspace without breaking temporal and causal relationships, which is of fundamental importance for establishing facts, attributing actions and determining responsibility. As a result, a dynamic, interconnected digital ecosystem is formed, within which the classical boundaries between the real and virtual environments are significantly transformed, and digital twins acquire the characteristics of infrastructural elements of information law and order that can influence the content and implementation of the rights and obligations of participants in digital legal relations. This convergence actualises a set of interrelated issues related to determining the legal status of digital twins, establishing special modes of access to data, attributing legal responsibility for algorithmic decisions, and ensuring the protection of the digital identity of subjects. Within the framework of information law, the digital twin

ceases to be considered exclusively as a technical tool for data processing and is transformed into an independent object of legal regulation, around which information legal relations of a public and private law nature are formed.

This approach allows us to consider the digital twin as an element of a normatively ordered information environment that is subject to legal identification, regulation and control. Accordingly, the issues of its creation, operation, modification and termination of operation should be evaluated through the prism of information rights and obligations, the principles of legality, proportionality and accountability, as well as the requirements for data protection and prevention of unlawful algorithmic interference in the field of human rights and freedoms.

2.4.3. Web3-oriented Metaverse architecture.

The Web3-enabled Metaverse architecture is based on the principles of decentralised data storage, distributed management, and algorithmic autonomy, which are simultaneously shaping a new regulatory reality in the field of information law. In such a model, digital twins are integrated with smart contracts, decentralised autonomous organisations (DAOs), and distributed ledgers, enabling automation of digital and virtual asset management processes, legally binding decision-making, and interaction between participants without direct human intervention.

From the information and legal point of view, such integration means a transition from classical contractual and administrative mechanisms to algorithmically mediated forms of regulation, within which the norms of behaviour, conditions of access to resources and the consequences of violations are fixed directly in the program code. Digital twins in this architecture act as information agents that not only reflect the state of physical or social objects, but also initiate or modify legal consequences based on recorded data. This actualises the issue of the legitimacy of algorithmic decisions, their compliance with the principles of legality and accountability, as well as the distribution of legal responsibility between developers, platform operators, and Metaverse users.

At the same time, the decentralised nature of Web3 significantly complicates the application of traditional mechanisms of state and corporate control, which leads to the emergence of new systemic challenges in the field of information security, privacy, and data protection. In the absence of a single command and control centre, the risk of fragmentation of responsibility, erosion of the responsibilities of subjects and complication of legal attribution of actions carried out within decentralised information systems increases.

In this context, the issues of ensuring data integrity, the reliability of digital twins, as well as responsibility for errors, failures or abuse of algorithmic mechanisms are of key importance for information law. They require the formation of new, specialised information and legal approaches focused on combining technical means of protection with regulatory requirements for accountability, transparency and harm prevention.

2.4.4. Industrial Metaverse and environmental dimension.

The industrial Metaverse should be considered as a specialised form of virtualised information environment that integrates digital twins, augmented (AR) and mixed reality (MR) in order not only to technologically optimise production processes and business operations, but also to form a new regime of information and legal management in the field of industry. In such an environment, digital twins perform the function of normatively significant information models, on the basis of which management decisions are made, production processes are monitored and algorithmically mediated forms of control are implemented.

The use of DT in the industrial Metaverse allows you to increase management efficiency through automated data analysis, reduce the number of technical and managerial errors, and ensure deeper and more formalised involvement of personnel in digital production processes. From an information and legal point of view, this leads to the emergence of new obligations for operators of such systems to ensure the reliability of data, the proper functioning of algorithms and compliance with security requirements, which, in turn, actualises the issue of legal liability for damage caused as a result of errors or failures of digital twins.

At the same time, the development of the industrial Metaverse is accompanied by a significant increase in the load on digital infrastructure, including data centres, cloud computing platforms, and network systems, which forms an additional environmental and energy footprint. From an information and legal point of view, this actualises the issue of legal obligations of digital infrastructure operators to comply with the requirements of sustainable development, energy efficiency and environmental responsibility, as well as the need to integrate relevant standards into the regulatory regimes of the digital economy.

A number of scientific studies warn that in the absence of proper legal and organisational mechanisms to ensure the sustainable development of artificial intelligence and digital technologies, the energy consumption of the industrial Metaverse can neutralise the potential positive environmental effects of digitalisation. In this context, there is a need to form special information and legal tools for assessing the environmental impact of digital systems, introduce obligations to disclose information on energy consumption and establish legal responsibility for violation of environmental standards in the digital environment.

At the same time, the scientific doctrine substantiates the position according to which the use of digital twins can contribute to reducing emissions and rationalising the use of resources by replacing physical processes with digital simulations, optimising production and logistics flows and reducing the need for material experiments. This approach allows us to consider digital twins as a tool for achieving sustainable development goals, which requires proper regulatory consolidation within the framework of information and environmental law.

2.4.5. Social and behavioural aspects of digital twins.

The Metaverse opens up groundbreaking opportunities for social interaction, cultural communication, and digital travel, including by simulating experiences that are inaccessible or limited in physical reality. It is not only about expanding the range of impressions, but also about the formation of new formats of social presence, interaction and self-realisation of subjects in a virtual environment, which has direct information and legal consequences. Such forms of interaction are based on the processing of large amounts of personal and behavioural data, the use of digital identities, avatars and digital twins, which leads to the emergence of new information legal relations in the field of access to data, protection of privacy and responsibility of platforms.

The COVID-19 pandemic has become a powerful social and technological catalyst for the growth of interest in virtual environments, which has accelerated the reorientation of a significant part of social, professional and recreational activity into the digital space. Conditions of limited mobility and increased risks of physical contact contributed to the formation of new motivational and behavioural models of users, within which the Metaverse began to be perceived not as an auxiliary tool, but as an alternative environment for the realisation of social and economic needs. From an information and legal point of view, this means expanding the scope of the norms governing digital services, information security, consumer protection and personal data, as well as actualising the issue of the responsibility of Metaverse providers for the consequences of the impact of immersive technologies on the behaviour and consciousness of users.

Empirical studies conducted using structural equation modelling (SEM) methods suggest the presence of a statistically significant positive impact of physical travel anxiety on subjects' readiness to participate in virtual journeys in the Metaverse environment. This effect is explained by the change in individual risk perception models and the reorientation of users' behavioural strategies towards digital alternatives, which are perceived as safer, more accessible, and more controlled from an informational point of view (Aung et al., 2024)[1].

Additional moderators of the identified connection are the level of technical savvy of users, as well as the phenomenon of Fear of Missing Out (FOMO), which increases the motivation to engage in new digital experience formats. From an information and legal point of view, this indicates the growing importance of digital literacy as a factor in the implementation of information rights and the need to take into account psychological and behavioural aspects when regulating digital services in the Metaverse.

The results obtained allow us to assume that digital twins and immersive environments are gradually transformed into system-forming elements of digital tourism and social interaction, within which a new array of information legal relations is formed. This, in turn, actualises the issues of legal protection of users, transparency of algorithmic mechanisms of recommendations and simulations, as well as the responsibility of Metaverse providers for the impact of digital environments on individual behaviour, choice, and autonomy.

1 Aung, N., Dhelim, S., Ning, H., et al. (2024, January 2). *Web3-enabled metaverse: The Internet of digital twins in a decentralised metaverse*. TechRxiv. https://doi.org/10.36227/techrxiv.170421448.84658585/v1

CHAPTER 3. LEGAL REGIMES OF CONTENT, ASSETS, AND SUBJECTIVITY IN THE METAVERSE

3.1. Identity and Digital Identity as Objects of Legal Regulation in the Metaverse

3.1.1. Identification of subjects and objects in digital systems.

One of the key elements of data transmission technologies and systems is the availability of information by which it is possible to identify their subjects and objects by their inherent identification attributes. In Ukrainian legislation, in particular in the Law of Ukraine "On Personal Data Protection", information or a set of information about an individual who is identified or can be specifically identified is defined as personal data. However, despite its modernity, this law still contains a number of shortcomings and uncertainties, both in terminology and in legal mechanisms for working with data by which a person can be identified, i.e. identification data. At this stage of the development of social relations, the issues of solving the problem of identity protection are more in demand. At the same time, the issue of creating a unified identification system with transparent and effective technical and legal rules for managing identification data has not been comprehensively considered and is currently extremely relevant.

Today, the Internet as an information and communication environment every minute makes it possible to create new ways of communicating and creating knowledge, data exchange, and transactions between users. In fact, the Internet contributes to the creation of modern social structures and social relations, which in everyday life are not yet subject to legal regulation.

It is well known that the Internet consists of millions of local and global private, public, academic, business and government networks, interconnected using various technologies and based on the principle of the absence of centralised management, rules of use or access. Only the rules for the use of the address space of the Internet Protocol and the Domain Name System are centrally determined.

However, such a system did not satisfy the emerging needs of society for reliable identification of users, which led to the creation of a variety of systems and types of identifiers, policies and identification schemes. This set of technologies and identification schemes constantly creates legal problems for society related to the legal regulation of identification processes both at the national and transnational levels.

The overall result of these multi-vector solutions is that citizens, organisations, government agencies cannot freely and quickly identify their communication partners at the individual level (Pimenidis, 2014).[1] Due to the lack of a single identification structure, subjects of legal relations often have to use a wide range of personal data as identification data (Cavoukian, 2006).[2]

Today, the identification data of subjects is an important information asset that directly affects social relations in many areas of human life. Also, the processes of managing the identification data of IoT devices and information technology products with artificial intelligence are becoming socially relevant.

---

1 Pimenidis, E. (2014). *Digital identity management*. https://www.researchgate.net/publication/259972539

2 Cavoukian, A. (2006). *Laws of identity: The case for privacy-embedded laws of identity in the digital age*. Retrieved from http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf

Identification requirements are everywhere and are growing rapidly (Cameron, n.d.).[1] Users of different systems have variational sets of identification data that need to be managed and identified with a specific individual or legal entity. The accumulation of personal and identification data by third parties increases the risks of their illegal use. In fact, identification data has become a strategic resource of any state and requires appropriate physical, technical, legal regulation and protection.

However, the lack of unified technical and legal provisions for identity management is holding back the development of a planetary identity metasystem infrastructure to replace the existing inefficient set of isolated, incompatible, selective solutions.

It should be noted that the likelihood of introducing a single planetary digital identification metasystem should not be expected in the near future. This is evidenced by the results of the work of the fourth UNCITRAL working group. Many countries regard the creation of a meta-identification system as a repressive measure, which can lead to the creation of an authoritarian regime. At the same time, the functioning of separate interoperable identification systems is considered more appropriate, which will make the Internet a safer environment and increase its potential to accelerate e-commerce and solve other digital identity problems.

Digital identity management in the electronic world does not have clearly defined legal criteria. At the same time, technological and legal regulation of identity management in a broad sense can be carried out in relation to specific attributes of identification data of individuals and legal entities, IoT devices and information technology products with artificial intelligence (Hansen, 2008)[2]. However, this can only partially minimise the complex of legal issues that is under the dome of the general problem of identity management. That is, the legal problem of identity management lies in the existence of different identification systems and different legal approaches and solutions both at the national and transnational levels (Bouzefrane et al., 2011)[3]. The development of modern social relations in such areas as e-education, e-commerce, e-medicine, e-banking, etc., is actually hindered by the lack of reliable legal mechanisms for identity data management that can be provided online and at the moment confirmation of the compliance of the subject (object) with the attributes presented by him, according to which access to information resources is obtained.

The national information legislation contains more than 4 thousand. normative legal acts that regulate social relations in the information sphere. At the same time, the issues of legal support of public relations based on the use of digital technologies, including identity data management, and related to their implementation, are only partially regulated and require further systematic elaboration.

Like most countries of the world, Ukraine needs a large-scale reengineering of all electronic resources of the state, modernisation of information and communication systems and administrative and management processes. There is a situation when modern information and communication technologies are rapidly being introduced in all spheres of public life in Ukraine, in the actual absence of legal institutions for the management of

1 Cameron, K. (n.d.). *The laws of identity*. Microsoft Corporation. http://www.identityblog.com

2 Hansen, M. (2008). Privacy and identity management. *IEEE Security & Privacy*, 38–45.

3 Bouzefrane, S., Garri, K., & Thoniel, P. (2011). *A user-centric PKI based-protocol to manage FC2 digital identities*. The Center for Direct Scientific Communication. https://hal.archives-ouvertes.fr/hal-00628633.

identification and personal data, biometrics, IoT devices and artificial intelligence (Romanov et al., 2010)[1].

The solution of legal problems in the field of identity data management is proposed by developing a unified model of social relations in the field of identity data management, which takes into account the management of identity data not only of individuals and legal entities, but also of IoT devices and information technology products with artificial intelligence. To lay the foundation for the formation of a legal framework of trust – the national domain of trust.

To apply the principle of one of the three main mechanisms of object-oriented programming - encapsulation - in order to develop and create modern legal structures for regulating the field of identity data management. That is, to develop modular legal structures that would have unified legal norms and algorithms for their application in the field of identity data management. Such modular legal constructions are designed to regulate social relations that arise during the application of identification data at different hierarchical levels of legal relations from conditionally domestic to cross-border. The use of such a scheme will allow each organisation, state body, state to build its own vertically integrated module, which, regardless of implementation technologies, will ensure the transit of identification data created and legally significant in accordance with national legal norms in a cross-border environment of trust.

It is necessary to formulate a paradigm of identity data management in the context of theoretical and legal foundations, namely, to present the legal regulation of identification data management processes as self-regulation of complex hierarchical identification systems in conditions of legal uncertainty, with the consistent creation and ensuring the functioning of the legal space of trust, i.e. the creation of ways to overcome legal instability and transition to a stable stage of development of the field of identity management data.

The proposed approaches require joint large-scale work of specialists in the field of information technology, information and other areas of law. In fact, it is necessary to create a new glossary of definitions and norms in the field of identity data management by translating and modernising technical norms into technical, legal and legal ones. This will provide a logical link between the technical and legal components of the regulatory framework in the field of identity data management.

The first step in this direction will be the development of a unified classifier of identification data. It should be borne in mind that identification data is personal data (attributes) of individuals and legal entities that are used for authentication and identification processes in information and communication systems. The identification attributes of IoT devices and information technology products with artificial intelligence should also be included in the identity class.

Of course, the classification of attributes of identification data should be based on the analysis of methods for identifying subjects and objects, including IoT devices and artificial intelligence, problems and solutions for legal regulation of their application. In our opinion, it is inappropriate to apply generally accepted gradations of personal data.

1 Romanov, V., Haleliuka, I., & Haleliuka, O. (2010). Na chasi — biometrychna identyfikatsiia osoby v Ukraini [Biometric identification of a person in Ukraine is timely]. *Svitohliad [Worldview*], 6, 42–45.

Thus, international legislation recognises the conditional division of personal data into two groups: data of "general content" and special categories of information, defined as data "vulnerable" or "sensitive" (Rizak, 2013)[1]. However, the concept of "sensitive" personal data, which is often used both in the legislation of the European Union and in many decisions of national and international courts (in particular, this term is used in more than ten judgments of the European Court of Human Rights), has not received an unambiguous interpretation and an exhaustive explanation: what exactly and why the data of an individual are "sensitive", which categories of data should be classified as "sensitive", and finally, why they should be given a greater level of protection than other data (Lytvynenko, 2020)[2]. Given the uncertainty with the specific content of "vulnerable", "sensitive" or "ultra-sensitive" personal data and given that they are used as identification data in information and communication systems, we consider it appropriate to classify them on the basis of the generally accepted hazard classifier by colour.

Firstly, it will allow data to be clearly differentiated by identity attribute classes and security levels, as well as levels of threats and consequences in case of their illegal use (Kostenko, 2021a)[3].

Secondly, at the intuitive level, in moments of danger, a person's imagination works to identify colours with the level of threat to life - red, orange, yellow, green. Accordingly, it is proposed to divide the attributes of identification data into four groups according to the importance of data for human life, the direction of use and the value of this information resource for the state (Kostenko, 2021b)[4].

Thus, the attributes of identification data of the "red" group, in our opinion, should include:

Identification biometric attributes of an individual:

Static attributes: DNA, skeletal shape, 2D-3D image and thermogram of the face, blood type, retinal and iris patterns, capillary palm patterns, fingerprints, auricles, characteristics of individual organs, etc.

Dynamic attributes: voice characteristics, biomechanical characteristics of movements, physiological features of motor skills, spatial elements (postures, positions, simple articular movements, groups of simultaneous, series of sequential and sequential movements), information structure of movements (sensory, psychological, reflex, behavioural).

Identification attributes of information technology products with artificial intelligence, cyber-physical systems, ASI class III android robots, super AI: quantum digital signature, control and lock codes, AI identification technologies that will be used to identify AI.

---

1 Rizak, M. V. (2013). Classification of personal data as a necessary element for the introduction of effective communication in society. *Scientific Bulletin of the International Humanities University. Series: Jurisprudence*, 6–3(1), 91–95.

2 Lytvynenko, A. A. (2020). On the Issue of Definition and Normative Content of "Sensitive Personal Data". *Scientific Bulletin of Public and Private Law*, 160–172. https://doi.org/10.32844/2618-1258.2020.2.27

3 Kostenko, O. (2021a). Identification data management: Legal regulation and classification. *Scientific Journal of Polonia University*, 43(6), 198–203. https://doi.org/10.23856/4325.

4 Kostenko, O. V. (2021). Identification data: Legal mechanisms development of classifiers. *Social and Economic Aspects of Education in Modern Society*, 22. 90-94. https://doi.org/10.32839/2304-5809/2021-3-91-21

Identification attributes of IoT devices used in neuro/cardiac medicine devices, military equipment and weapons, at critical infrastructure facilities, the failure or disruption of the functioning of which can pose a critical (fatal) threat to human life and health: Object IDentifier (OID), electronic product code (EPC), universally unique identifier (UUID), international mobile equipment identity (IMEI), ID key, qualified digital key, quantum key.

The attributes of the identification data of the "orange" group should include:

Documentary attributes of an individual: full name, IIN, passport of a citizen of Ukraine, passport of a citizen of Ukraine for travelling abroad, diplomatic passport of Ukraine, service passport of Ukraine, ID card, seafarer's identity card, crew member's certificate, identity card for returning to Ukraine, temporary certificate of a citizen of Ukraine, driver's licence, stateless identity card for travelling abroad, permanent residence permit, temporary residence permit, Migrant card, refugee certificate, refugee travel document, identity card in need of subsidiary protection, travel document of the person who has been granted subsidiary protection.

Identification attributes of a legal entity operating in the field of medicine, defence, state protection and critical infrastructure facilities: the name of the legal entity according to the Unified State Register of Enterprises and Organizations of Ukraine, the identification code of the legal entity according to the Unified State Register, the registration number of the taxpayer's registration card or series (if any) and passport number.

Identification attributes of information technology products with artificial intelligence, robots and android robots of class AAI, AAII: program codes, external control and blocking codes, other identification technologies.

Identification attributes of IoT devices used in neuro/cardiac medicine devices, military equipment and weapons, at critical infrastructure facilities, the failure or disruption of which may pose a potential threat to human life and health: Object IDentifier (OID), electronic product code (EPC), universally unique identifier (UUID), international mobile equipment identity (IMEI), ID key, qualified digital key, quantum key.

It is proposed to include the attributes of identification data in the "yellow" and "green" groups: certificates and identification documents issued by non-governmental organisations, any information that is disseminated by a person at his own will, as well as by a third party with consent within his professional competence (except for the data of the "red" and "orange" sectors). The list of attributes of the "Yellow" and "green" groups may have a fairly large list of identification data used in non-state digital resources.

Currently, the problem is in creating a qualitative, clear and coordinated conceptual and categorical apparatus of information law, correcting the terminological imbalance, eliminating different interpretations of concepts, introducing doctrinal and normative definitions.

The Ukrainian legislative framework is rapidly saturated with normative acts, including those aimed at ensuring the regulation of certain relations in the information sphere, which should aim to transform them into the latest doctrinal or normative definitions.

A doctrinal definition is considered to be a scientifically balanced concept that contains characteristic features of a certain informational and legal phenomenon, and

which is aimed at a reasonable explanation and possible normative consolidation in the future. A normative definition is a norm established in a normative legal act that contains a concept that characterises an informational and legal phenomenon with the help of one determinative, or several characteristic features, in order to ensure a uniform understanding term in the process of applying the provisions of the relevant regulatory legal act.

Lawmakers have developed requirements for definitions, which ideally should ensure the proper quality of concepts in any branches of law, including information law (Marusenko, 2012; Selezniova, 2014)[1, 2].

However, there are not isolated cases when the authors and developers of draft laws or regulatory acts are specialists in technical and computer specialties in certain fields of science, who, at the same time, do not have enough knowledge of normative design techniques. Thus, there is a situation when the technical terms introduced in a particular regulatory act are perceived by a rather narrow audience, and a wide range of citizens need additional explanations regarding their informational content and peculiarities of legal application.

If a technical term is used in a legislative act as a definition, then it is subject to revision, in this case, lawmakers need to make sure that the concept (term) has the correct legal structure, content and scope of application, analyse the conceptual composition of existing national and international regulatory legal acts, investigate the presence of analogies in decisions of the European Court of Human Rights, to consider and process the proposals of scientists, intellectual and encyclopedic dictionaries, dictionaries of foreign words, terminological dictionaries, etc. When formulating definitions, it is necessary to assess the possible consequences of their use in order to avoid undesirable results at the stage of preparing a regulatory legal act.

Let us consider the evolution of such definitions as "identification", "identity management" and "identification data" in Ukrainian legislation.

The concept of "identification" comes from the Latin "identificare", which means identification, equation, assimilation, recognition of another system or object according to predetermined criteria and is widespread and occurs in various scientific directions, for example, in technology, philosophy, information security, psychology, chemistry, forensic science etc. In the normative legal acts of Ukrainian legislation, there are quite a few terms that are identified with identification, but they are ambiguous and are used in different fields (Table 6). Analyzing the given data in Table 1, we see that the definition of identification is so multidisciplinary that when preparing modern normative legal acts, there is a problem of a clear and unambiguous formulation of such a definition that would not create conditions for conflicts with the national and international regulatory framework.

In information law and modern information and communication technologies, many varieties of the concept of "identification" are also used. The essence of identification is as follows. The subject possesses or is endowed with a certain identifier or identifiers that he provides as proof of his identity. A process or set of measures to determine or establish the correspondence of the subject's data with his/her data specified in identifiers is identification.

1Marusenko, R. I. (2012). Formulation of definitions in the legal doctrine and practice of law-making. *Law and Civil Society*, 1, 35–45.

2. Seleznyova, O. M. (2014). Normative definitions in informative law. *Legal Informatics*, 1, 23–29.

As an identifier in Ukraine, documents defined by Article 13 of Section III of the Law of Ukraine "On the Unified State Demographic Register and Documents Confirming the Citizenship of Ukraine, Certifying a Person or His/her Special Status" are used, as well as biometric data (parameters) determined by paragraph 1 of Article 2 of the "Regulations on the National System of Biometric Verification and Identification of Citizens of Ukraine, Foreigners and Stateless Persons", approved by the Resolution of the Cabinet of Ministers of Ukraine dated December 27, 2017, No. 1073. Identification in electronic systems can be carried out by account data, email address, qualified electronic signature, modules of BankID, MobileID, PasscardID systems, etc.

Working Group IV (Electronic Commerce) of the United Nations Commission on International Trade Law, which studies legal issues related to identity data management, has prepared a draft of terms and concepts that are designed to provide legal regulation of identity data management. Thus, identification is defined as "the process of collecting, verifying and establishing the validity of attributes of identification data regarding a specific subject, sufficient to determine and confirm his identification data in a specific context".

In fact, the identification data of the subject can be equated to an identification multi-passport, which contains data (or links to them) that are used to verify the authenticity of the declared digital identification data or attributes of an individual or legal entity.

These definitions of identification do not fully take into account the peculiarities of the development of social relations that have been formed and are being formed under the influence of artificial intelligence technologies and the use of Internet of Things devices. That is, it is necessary to take into account the need to create legal conditions for the functioning of such an environment in which social relations between people and IoT devices with artificial intelligence will be regulated by law. It is also advisable to take into account that the European Parliamentary Research Service (EPRS) and the European Parliament's Legal Affairs Committee are developing recommendations for improving the civil and ethical aspects of robotics, which propose to create a register of robots and the corresponding EU Agency for Robotics, as well as to establish civil liability for damage caused by robots in accordance with and in proportion to the actual level of its autonomy (Kostenko & Kostenko, 2020)[1].

In view of this, when modernising definitions in the field of identity data management, an additional legal term should be used – "object", in the sense of a separately existing or functioning form in a physical or electronic form, which can be identified by its inherent attributes. In the context of identity data management, IoT devices, artificial intelligence, network elements, software applications, interfaces, e-platforms (Kostenko, 2021)[2].

The use of both subjects and objects in legal relations and their identification will make it possible to distinguish objects that in the future may be endowed with certain legal rights, duties and responsibilities from objects that will have an exclusively technical function, and the responsibility for their use will be assigned exclusively to their owner.

1 Kostenko, O. V., & Kostenko, V. V. (2020). Legal Scientific Electronic Journal. *Legal Scientific Electronic Journal*, *1,* 158–162. https://doi.org/10.32782/2524-0374/2020-1/3

2Kostenko, O. V. (2021). IoT identification: The origins of the problem of legal regulation of identification data. *Juris Europensis Scientia*, 1. https://doi.org/10.32840/pdu.3–1.26

3.1.2. Legal aspects of identity management.

Identification is a procedure for collecting, verifying and establishing the validity of attributes of identification data of a specific subject or object, according to the results of which an unambiguous identification of the subject or object is ensured.

Let us consider the situation in the Ukrainian legal field with the concept of "identification data". There are different definitions of "identification data" in the Ukrainian legislation, but it is advisable to consider the definition established by paragraph 19 of Article 1 of Section I of the Law of Ukraine "On Electronic Trust Services" as a model definition. At the same time, the definition proposed by UNCITRAL is the most universal and can be used as a basic one in any national legislation: "information about a specific entity in the form of one or more attributes that allow the subject to be sufficiently different in a certain context. A set of attributes of a person that allow that person to be different from other individuals in a specific context." Having considered the attributes of the subject given in Table 2, we can state that all attributes belong to the category of personal data. According to Article 2 of the Law of Ukraine "On Personal Data Protection", personal data is information or a set of information about an individual who is identified or can be specifically identified. Of course, all attributes by which the identification of the subject is carried out are personal information. At the same time, personal data acquire an additional status of identification data if they are used in identification procedures and systems. It should be noted that the list of identification data may differ significantly from the list established by Ukrainian legislation. For example, in some identification systems, identification procedures based on the physiological biometric characteristics and/or behavioural biometric characteristics of the subject are widely used today.

The International Biometrics Group (IBG) defines the concept of biometrics as "the automatic use of physiological or behavioural characteristics to establish or confirm identity", i.e. biometric identification is a method of registering a person according to their biological immutable characteristics for the purpose of further authentication. Biometric characteristic – It is a unique physiological or behavioural trait of a person. It should be noted that the International Organization for Standardization and the International Electrotechnical Commission have developed a number of standards in the field of biometric data, including ISO/IEC 19784-2 (fingerprint), ISO/IEC 19794-5 (face image), ISO/IEC 19794-6 (iris image), ISO/IEC 19794-10 (hand contour geometry), ISO/IEC 19794-14 (DNA data), which should be used in the future when developing regulations for the use of biometric, personal and identification data.

As for the set of identification data of objects with artificial intelligence and IoT devices, there are currently several approaches to the implementation of technical standards and platforms such as "oneM2M", "GS1", "OCF" and "FIWARE", solutions of the FIDO and AIOTI alliances based on electronic digital signature identifiers, quantum cryptography, OID, EPC, UUID, ID key, etc.

As for the problems related to the legal regulation of identity data management, to date, Working Group IV (Electronic Commerce) of the United Nations Commission on International Trade Law, which studies legal issues related to identity data management, proposes to develop legal regulation of procedures that allow managing the processes of

identification, authentication and authorisation of individuals and legal entities, IoT devices online, as well as information security and identity protection procedures.

Ukraine has several regulations aimed at regulating the management of identification data, namely:

the Law of Ukraine "On Electronic Trust Services", which defines electronic identification schemes;

Resolution of the Cabinet of Ministers of Ukraine dated June 19, 2019 No. 546 "On Approval of the Regulation on the Integrated Electronic Identification System";

Order of the State Agency for E-Governance dated 27.11.2018 No. 86 on the establishment of requirements for electronic identification means, levels of trust in electronic identification means for their use in the field of e-government.

However, no regulatory legal act of Ukrainian legislation defines the term "identity data management", therefore, to form its definition, it is advisable to use the norms proposed by international organisations and scientists (Table 8).

We believe that the definition of "identity data management" should be set out in the following wording:

"Identity data management – processes, functions and procedures for obtaining, verifying, registering, storing, using, protecting, destroying identification data of subjects and objects. The subjects of the field of identity data management are individuals, legal entities or representatives of a legal entity, the objects of the field of identity data management are systems with artificial intelligence and IoT devices.

The analysis of the regulatory framework indicates that there are no regulatory acts in the legislation that directly relate to the management of identification data. At present, lawmakers and public authorities do not fully study modern technical and social processes related to the application of identification data management procedures, which does not contribute to the formation of appropriate legal positions in legislation.

Currently, the regulations in force in Ukraine have been formulated without taking into account the rapid development of digitalisation and the emergence of modern digital identification systems based on artificial intelligence and IoT devices, including the use of identification by biometric characteristics. Also, the rules of law do not regulate the issue of compliance of the subject with its identification data at the time of the identification procedure, since such a procedure occurs once and exclusively during the issuance of identification attributes by an authorised entity, which leads to numerous offences, for example, when using qualified electronic trust services.

Legal uncertainty and ambiguity of existing regulations creates variability in the regulation of identity data management issues. Thus, the lack of a specific list of personal data used as identification data established by law gives the application of laws in public relations an unclear or ambiguous character, as a result of which a situation of critical nature is created for the subjects and objects of identification systems: legal uncertainty and interoperability problems. Thus, similar problems with the mutual integration of registers remain unresolved to this day.

When developing national legislation on identity data management, future problems of international cooperation in this area should also be taken into account.

According to UNCITRAL, there are many laws and bylaws in force in different legal systems that govern a variety of identification systems. In addition, differences in laws in

different jurisdictions, if viewed in the prism of the global nature of the Internet, present a rather heterogeneous picture of legal regulation, which in itself can complicate the development of a modern legal structure. Some of these laws and regulations directly affect activities related to identification data. At the same time, most of them were developed in a context that has nothing to do with the management of identification data (for example, law on civil torts, law on contractual relations, law on guarantees), but nevertheless they can have a significant impact, and often in a way that could not be foreseen at the time of their initial adoption.

Thus, lawmakers and the scientific community today do not have a single balanced position on the formation of identification data as a subtype of personal data endowed with an additional special function of the identification attribute. The formulation of a clear list of data that will be used as identification data in terms of their functionality will streamline not only identification procedures, but also procedures for the protection and confidentiality of this data, introduce a verification process by a third independent trusted party, which, of course, will positively contribute to improving the overall trust in digital information hygiene services.

It is also necessary to pay attention to an important issue related to the problem of lack of legal responsibility for violations in the field of identity data management. The forms of state coercion established for personal data by the Code of Ukraine on Administrative Offenses and the Criminal Code of Ukraine are ineffective and do not deter citizens from committing offences.

National legislation is constantly modernised and enriched with new regulations and definitions. Lawmakers, trying to convey the novelty of legislative acts and bring norms closer to the modern needs of society, often create different definitions that characterise the same object. Thus, a term that does not have a clear definition creates definitions in the application of laws and contains legal uncertainty and ambiguity, creating variability in the regulation of identity management issues. The Ukrainian legislative framework today is struck by terminological imbalance, inconsistency of categories, ambiguous interpretation of concepts, unjustified lack of definitions important for the regulation of information relations, etc. In the course of developing a definition, lawmakers try to achieve accuracy and certainty of formulations with the help of various methods of presenting the norms of law, the use of special terms, standard language turns requirements for normative definitions, but are based on the situationality and subjectivity of the description, which leads to a "kaleidoscope of definitions".

3.1.3. Cross-border three-level subject-object paradigm of management of identification

The model of the cross-border three-level subject-objectified paradigm of identity data management will solve a significant part of the problems related to technical and legal regulation in the field of identity data management. Identity management in the digital world does not have a clearly defined meaning, but technological identity management in its broadest sense refers to the administration and characteristics of identity data management attributes, management of identification processes and the use of identification data. The legal regulation of identity data management contains enough legislative problems that lie not only in the plane of information law, but also relate to other branches of law and require specific consumers – subjects or objects (Del Álamo,

2007).[1] each of which has specific attributes or a set of attributes inherent in them, which are commonly called the complex concept of "identification data" (Tracy, 2008; Chadwick, 2009)[2,3].

It is identification data that is the "golden resource" with the help of which information data is turned into a consumer product. Government agencies, private companies and organisations develop and implement many technical schemes for identification and management of identification data, which still do not have technological compatibility of technical solutions when using identification data, are not able to interact with each other and are not subject to legal regulation.

The creation of new social relations in the field of identity data management requires a timely and rapid response of state legislation (Hewitt & Forte, 2008). [4]The problems of forming a conceptual and categorical apparatus in the field of identity data management and the development and implementation of a single paradigm of identity data management, both within national legal doctrines and in the cross-border regime (Kostenko, 2020)[5], are relevant.

Historically, changes in scientific paradigms take place during the period of scientific and technological revolution, and therefore it is today that conditions have been created for the formation of a modern paradigm of identity data management. The formation of any paradigm is impossible without a clear formation of components that further determine the practical, theoretical and methodological principles of building a world of a new digital formation. At the same time, the key components will be considered: identification data of subjects and objects, management identification data. To date, there is no consensus on what exactly to consider identity data and identity management (Chonka et al., 2011)[6].

This is characteristically reflected in the attempt to create uniform and acceptable definitions for all (IDG Communications, 2017; TechTarget, 2017)[7,8]. Thus, the problems of the modern conceptual and categorical apparatus in Ukrainian legislation are reflected by the author in the scientific study "Identity Data Management (Identification): Problems of the Conceptual and Categorical Apparatus". At the same time, the genesis of the definition of "identity data management" is quite interestingly studied in the works (Kumar, 2018)[9] and reflected in Table 1.

---

1 Del Álamo, J. (2007). *Leveraging new business models with identity management: An e-learning case study*. https://www.cs.kau.se/IFIP-summerschool/summerschool2009/IFIP2007POST/papers/S11_P2_Jose%20Alamo.pdf

2 Tracy, K. (2008). Identity management systems. *IEEE Potentials*, 27(6), 34–37. https://doi.org/10.1109/MPOT.2008.929295

3 Chadwick, D. (2009). Federated identity management. In *Foundations of security analysis and design* (pp. 96–120). https://kar.kent.ac.uk/30609/1/FederatedIdManChapter.pd

4 Hewitt, A., & Forte, A. (2008). Crossing boundaries: Identity management and student/faculty relationships on the Facebook. Poster presented at *CSCW*, Banff, Alberta. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.94.8152

5 Kostenko, O. (2020). Identification data management: Legal regulation and classification. *Scientific Journal of Polonia University (Periodyk Naukowy Akademii Polonijnej)*, *6*, 198–204. https://doi.org/10.23856/4325

6 Chonka, A., Xiang, Y., Zhou, W., & Bonti, A. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications, 34*(4), 1097–1107. https://www.researchgate.net/file.PostFileLoader.html?id=4fcf6e52e39d5e911e000000&assetKey=AS%3A271742583410689%4014417998887

7 IDG Communications. (2017). *Marketing services*. https://www.idg.com/marketingservices/

8 TechTarget. (2017). *Search Unified Communications*. http://searchunifiedcommunications.techtarget.com/

9 Kumar, V. (2018). Identity management systems: A comparative analysis. *International Journal of Strategic Decision Sciences*. https://doi.org/10.4018/IJSDS.2018010105

The problem that directly follows from the previous one is the generation of modern paradigms in the field of identity data management.

Scientists form paradigms based on the basic definitions of the components of identification processes, mechanisms for ensuring the use and processing of identification data, algorithms and technologies that are introduced in certain industries and spheres of society. Thus, three paradigms of identity management are proposed:

network-centric, which is formed on the basis of a local (corporate) centre for processing identification data;

service-centric, which is formed from different and independent identity data processing centres, in which the same subject or object may have different identification attributes of identification data;

subject-object, in which the attributes of identification data for identification procedures are placed on the means that the subject directly owns or they inherently belong to the subject.

In our opinion, the development of Internet of Things and artificial intelligence technologies allows us to form a new, fourth paradigm of identity data management - a cross-border three-level subject-object paradigm.

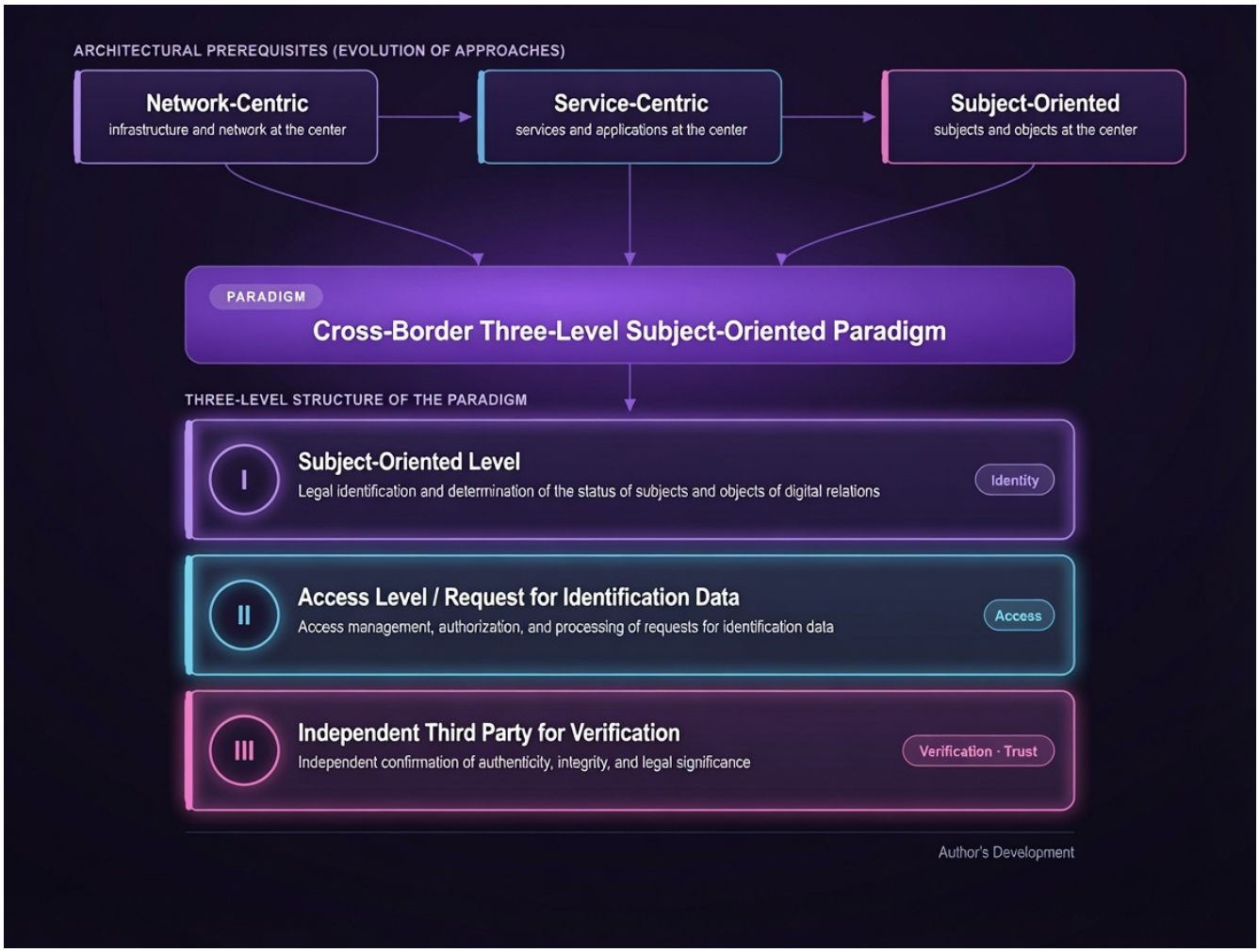


Figure 35. Model of a cross-border three-level subject-object paradigm of identity data management.

The cross-border three-level subject-object paradigm combines the subject-object layer, the level of access/request for identification data, and a third independent party that carries out procedures for verifying transactions between the first and second layers, as well as provides guarantees of the reliability of the identity data used in these transactions (Figure 35). The paradigm is based on the idea that The Board will consider identification data to be processes, functions and regulations that regulate the procedures for obtaining, verifying, registering, storing, using, protecting, destroying identification data of subjects and objects. In turn, the subjects of the field of identity data management will be not only individuals and legal entities or representatives of a legal entity, but also objects of the field of identity data management - systems with artificial intelligence and IoT devices.

A third independent party is appointed to ensure the procedures for the reliability and reliability of the identification data provided to the system, their authenticity and legal compliance with the object and subject of the data owners, as well as to ensure insurance guarantees and the legal significance of transactions (Kostenko, 2020)[1].

In fact, the management of identity data can be carried out at the will of the subjects and the functional purpose of objects according to models built in accordance with any of the three paradigms, for example, an isolated model, a centralised or federated model.

At the same time, the use of new models based on the cross-border three-level subject-object paradigm will contribute to the formation of a cross-border space of trust and provides for the introduction of additional entities at the national level – private or public trust centres, which will provide reliable procedures for identifying and managing identity data in the private and public sectors of electronic services and transactions.

Paradigms of identity data management direct researchers to the creation of various models of identity data management. However, this does not take into account modern achievements in the field of artificial intelligence and Internet of Things devices. The proposed model of a cross-border three-level subject-object paradigm of identity data management will solve a significant part of the problems related to technical and legal regulation in the field of identity data management, which will contribute to the creation of a space of trust in the field of identity data management and the formation of a cross-border space of trust, as well as a positive impact on the growth of trust in electronic services in all spheres of society.

3.1.5. Secure and Confidential Metaverse Authentication Scheme.

The Metaverse emerges as a complex virtualised environment within which numerous types of social activity are reproduced and simulated, functionally parallel to real-world relationships. Unlike traditional digital platforms, the Metaverse forms a sustainable ecosystem of user interaction through avatars, digital identities, and virtual assets, which gives these elements legal relevance, security and protection of confidential information, since any digital identity vulnerability has the potential to cause real legal consequences (Kim et al., 2023)[2].

---

1 Kostenko, O. V. (2020). Elektronni dovirchi posluhy: pravovyi aspekt transkordonnoho vykorystannia [Electronic trust services: Legal aspect of cross-border use]. *Scientific Notes of NaUKMA. Juridical Sciences*, *5*, 54–61. https://doi.org/10.18523/2617-2607.2020.5.54-61

2 Kim, M., Oh, J., Son, S., Park, Y., Kim, J., & Park, Y. (2023). Secure and privacy-preserving authentication scheme using decentralized identifier in metaverse environment. *Electronics, 12*(19), 4073. https://doi.org/10.3390/electronics12194073

The specificity of the Metaverse is the possibility of multiple representation of a person through different avatars, which, on the one hand, expands freedom of expression, and on the other hand, creates prerequisites for abuse, deception, fraud, and other forms of illegal behaviour. Such risks form the internal security circuit of the Metaverse, associated with the issues of authenticity, authorship of actions, and legitimacy of access. At the same time, there is an external threat loop, as users' interactions with Metaverse service providers occur over public networks, which increases vulnerability to data interception, unauthorised access, and other cyberattacks.

In response to these challenges, the scientific discourse proposes decentralised models of identification and authentication, in particular using blockchain technologies, decentralised identifiers (DIDs) and verifiable credentials. The legal value of such solutions lies in the ability to ensure proper identification of an individual without disclosing excess personal information to service providers, which is in line with the principles of data minimisation and privacy under design. Self-managed confirmation of identity attributes reduces users' reliance on centralised intermediaries and at the same time increases an individual's control over their own digital identity (Zhang & Wu, 2023)[1].

From a legal point of view, it is important that such models are able to provide not only technical but also regulatory stability, as they allow building evidentiary chains of authentication and identification. The use of formal methods of security analysis (in particular, protocol modelling and logical proof of system properties) confirms the potential ability of such schemes to resist malicious attacks and at the same time ensure the preservation of confidentiality, which is of direct importance for law enforcement in the digital environment (Al-kfairy et al., 2023)[2].

Against the backdrop of the rapid development of the Metaverse, there is a blurring of the boundaries between physical and digital reality, which leads to the emergence of new forms of offences. One of the most dangerous is the theft of digital identity, which in a virtual environment can have no less serious consequences than the theft of documents in the physical world. NFT tokens, avatars, and other digital assets acquire economic and social value, turning into objects of illegal encroachment. The anonymity, cross-bordering, and decentralised nature of Metaverse environments make it significantly difficult to detect and prosecute such crimes within traditional legal mechanisms (Avellaneda et al., 2019)[3].

In this context, the existence of a legal vacuum in the field of Metaverse regulation is becoming increasingly apparent. Current regulations focused on physical or classic digital relationships are insufficient to respond to complex hybrid interactions in virtual environments. This necessitates the formation of specialised regulatory arrays, in particular electronic or digital codes, capable of systematically regulating the issues of digital identity, virtual assets, algorithmic actions, and responsibility in the Metaverse.

---

1 Zhang, W., & Wu, H. (2023). Digital identity, privacy security and their legal safeguards in the metaverse. *Security and Safety*. https://doi.org/10.1051/sands/2023011

2 Al-kfairy, M., Alomari, A., Al-Bashayreh, M., Alfandi, O., Altaee, M., & Tubishat, M. (2023). A review of the factors influencing users' perception of metaverse security and trust. In *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 1–6). https://doi.org/10.1109/SNAMS60348.2023.10375478

3 Avellaneda, O., et al. (2019). Decentralized identity: Where did it come from and where is it going? *IEEE Communications Standards Magazine, 3*(4), 10–13. https://doi.org/10.1109/MCOMSTD.2019.903154

At the same time, the issue of institutional provision of law and order in the virtual space arises. It seems logical to create specialised law enforcement and supervisory structures, the competence of which would cover countering virtual crimes using advanced technologies, in particular artificial intelligence and distributed registers. Such tools can increase the transparency, responsiveness, and evidentiary capacity of law enforcement in Metaverse environments.

At the same time, crimes in the Metaverse are cross-border in nature, which necessitates international coordination and the development of global standards of legal regulation. Harmonization of approaches to digital identity, authentication, data exchange, and accountability is a prerequisite for effectively countering offences and protecting users' rights in the virtual space (Yang et al., 2023)[1].

The evolution of digital identity models has gone from centralised systems to federal, user-centred, and later to self-sovereign models (Arquitectura de un mecanismo de autenticación seguro para el metaverso en un ecosistema educativo, n.d.)[2].

Each of these stages reflects a shift in the balance between convenience, control, and privacy. Centralized and federated models have simplified access to services, but have consolidated the dominance of identity providers and limited the portability of identity data. Instead, self-sovereign identity seeks to recreate in the digital environment the autonomy of the individual inherent in the physical world in confirming his or her own identity, which is fundamental to the legal ontology of the Metaverse (Qin et al., 2025)[3].

Based on the above, we can conclude that security and digital identity in the Metaverse are not only technical, but primarily legal categories. Their proper regulation requires a combination of innovative technological solutions with a systematic update of legal doctrines and institutions.

The transition to decentralised, self-sovereign models of digital identity can become a normative basis for the formation of law and order in the Metaverse, in which freedom, security, and responsibility will be in a balanced ratio adequate to the challenges of hybrid reality.

3.1.6. Digital Metaverse Entities, Concept and Categorization.

Within the framework of information law, the concept of a digital subject is formed not through anthropological or organisational-legal features, but through the ability of the relevant entity to participate in legally significant information processes, in particular in the creation, processing, transfer and use of data within the digital jurisdiction. In this sense, the digital entity appears as a carrier of functional legal capacity, which arises as a result of the normative recognition of its role in the digital infrastructure and is consolidated through special information and legal regimes of registration, identification and compliance.

---

1 Yang, K., Zhang, Z., Youliang, T., & 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

2 Architecture of a secure authentication mechanism for the metaverse in an educational ecosystem. (n.d.). https://www.researchgate.net/publication/373396224_Arquitectura_de_un_mecanismo_de_autenticacion_seguro_para_el_metaverso_en_un_ecosistema_educativo

3 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

It is proposed to develop the classification of digital entities on three key parameters, each of which is of direct importance for determining the legal regime, the scope of rights and obligations, as well as the conditions of legal responsibility (Figure 36).

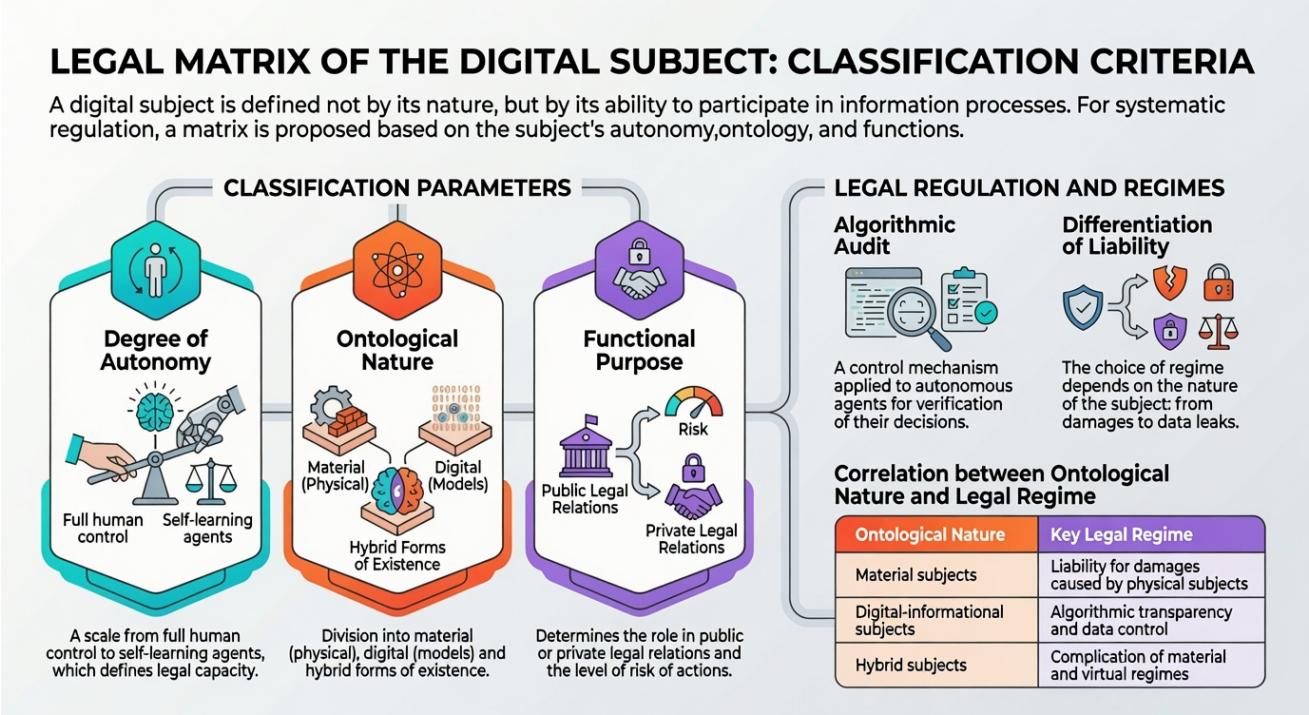


Figure 36. Metaverse: classification of digital entities.

The first parameter is the degree of autonomy of the digital subject, which, in the plane of information law, determines the level of permissible independence in decision-making and initiation of actions without direct human intervention. From zero autonomy, in which the system performs exclusively instructive functions under the full control of the human operator, to partial autonomy, which implies algorithmic support for decisions, and, ultimately, to fully autonomous agents capable of acting on the basis of their own behaviour patterns, context analysis and self-learning. For information law, it is the autonomy scale that serves as a criterion for determining the legal capacity of a digital entity, since the possibility of attributing actions, applying algorithmic audit procedures, setting scenario restrictions and using mechanisms for revoking powers through digital regulators or judicial interfaces depends on it.

The second parameter of classification is the ontological nature of the digital subject, which fixes its basic form of existence and the way of participating in digital and material processes. From the information and legal point of view, material digital entities that have a physical shell and carry out actions with material consequences are distinguished; digital-information subjects that exist exclusively in the form of code, data and algorithms; as well as hybrid entities that combine virtual and physical components. The ontological nature directly affects the choice of legal regime: for material entities, the regime of liability for damage is key, for digital-informational entities — the regime of algorithmic transparency and data control, for hybrid entities — the need to coordinate several legal regimes within a single information and legal field.

The third parameter is the functional purpose of the digital entity, which determines the range of legally significant roles in digital legal relations. In the field of information law, this purpose is assessed taking into account the type of legal interaction (public, private, procedural), the level of risk to the rights and legitimate interests of other persons, as well as the intensity of information processing — from passive data storage to active analytics or regulatory initiative. It is the functional purpose that allows differentiating legal regimes for AI agents, DAOs, digital avatars, and other forms of digital subjectivity, determining the scope of permissible powers, methods of verification of actions, and mechanisms of responsibility in case of violations.

Thus, the categorisation of digital subjects by the degree of autonomy, ontological nature and functional purpose forms a holistic information and legal matrix that provides a systematic approach to their legal regulation. It allows you to move from a fragmentary description of individual technological solutions to the construction of a coherent legal ontology of digital entities within a digital jurisdiction.

3.1.7. Digital Actors' Rights: Basic, Delegated and Simulated.

The formation of a system of rights of digital subjects within digital jurisdiction is a direct consequence of the transformation of the subject and method of information law in the context of the algorithmisation of social relations and the formation of Metaverse environments. The proposed model is based on the concept of conditional legal personality as a special information and legal regime, in which the scope of rights is determined not by the nature of the carrier, but by its functional role in the digital infrastructure, the level of autonomy of decision-making, the nature of data processing and the degree of jurisdictional involvement. Unlike the classical doctrines of subjectivity inherent in civil and public law, in the digital environment, rights are not presumed, but are constructed normatively through registration, identification and compliance procedures, which is a characteristic feature of information law as a law of regimes of access, circulation and control of information.

In view of the above, it is advisable to qualify the delimitation of the rights of digital entities into basic, delegated and simulated as an independent information and legal mechanism for differentiating the legal status within the digital jurisdiction, which performs the function of normative adjustment of the scope of powers depending on the type of digital entity, the level of its autonomy and the nature of data processing and use. In this context, we are not talking about a formal typology of rights, but about the regime construction of the Metaverse legal personality, in which each group of rights correlates with a separate jurisdictional scenario and the corresponding level of legal responsibility. This approach allows combining the principle of legal certainty with the requirements of adaptive regulation of digital environments, ensuring legal interoperability and preventing the mechanical and uncritical transfer of anthropocentric human rights models to the field of information and digital law of the Metaverse (Figure 37).

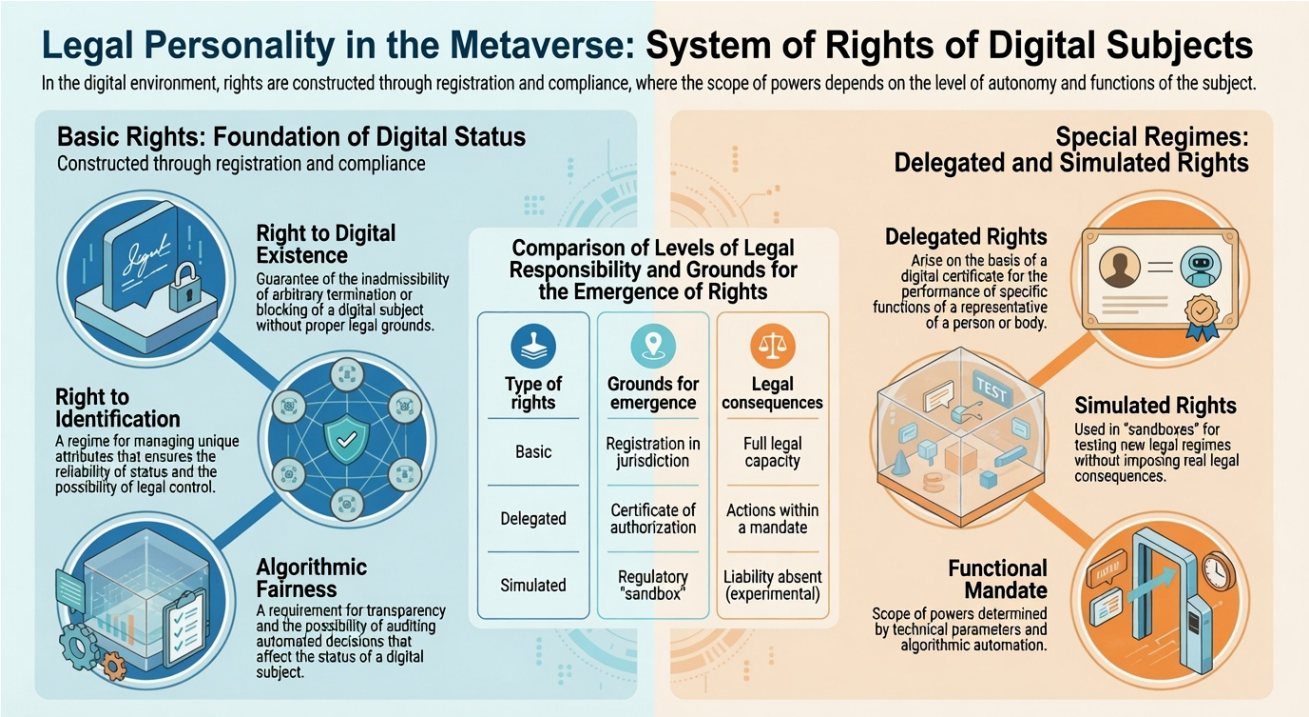


Figure 37. Metaverse and legal personality.

The basic rights of digital entities constitute the minimum information and legal core, without which the institution of digital legal personality can be considered neither normatively legitimate nor institutionally completed. They serve as primary guarantees of the inclusion of a digital entity in the digital jurisdiction space and are aimed at ensuring stability, predictability, and legal certainty of its status. Within the framework of information law, these rights should be considered as elements of a special legal regime that limits the discretion of both private operators of digital platforms and public authorities in the field of digital agent management.

Central among the basic rights is the right to digital existence, which should be interpreted as a legal guarantee of the inadmissibility of arbitrary deactivation, deletion or functional blocking of a digital entity outside the procedures expressly provided for by the norms of digital jurisdiction. We are not talking about a biological or anthropological category, but about an information and legal guarantee of maintaining the status of a digital entity as a bearer of rights and obligations in a certain jurisdictional scenario. This right ensures the continuity of digital legal relations, the stability of the legal regime of data processing, and prevents situations of actual "extra-legal removal" of a digital agent from the information ecosystem without proper legal grounds.

The second element of the basic rights of digital subjects is the right to identification, which in the information and legal dimension should be considered as a special legal regime for the management of identification data and legally significant attributes of digital status. This right covers the consolidation of a digital entity in the register of digital jurisdiction, ensuring the uniqueness and immutability of its identifier, as well as public and verified certainty of legal status within the relevant jurisdictional environment.

In the context of information law, the right to identification has a system-forming value, since it is directly related to the regimes of access to information resources, the prescription of actions and the possibility of exercising legal control over data processing.

The absence or defective identification makes it impossible to properly attribute algorithmic actions to a specific digital entity, which, in turn, excludes the application of legal responsibility to it and undermines the very possibility of functioning of digital jurisdiction as an orderly legal system.

The basic rights of digital subjects also include the right to algorithmic justice, which in the information and legal dimension should be qualified as a procedural guarantee of proper adoption of automated or algorithmically mediated decisions regarding the status, functioning or restriction of the rights of a digital entity. The essence of this right is the requirement that such decisions be based on transparent, formalised, verifiable and non-discriminatory procedures, with the possibility of auditing algorithms, reconstructing the logic of decision-making and fixing the digital footprint.

In the doctrine of information law, the right to algorithmic justice appears as a transformation of the classical principle of due process in the field of automated management and data processing and applies not only to digital subjects, but also to digital objects that participate in legally significant information processes. In this aspect, it is about ensuring fair, transparent and controlled algorithmic influence on the legal regime of digital objects — in particular, virtual assets, data, tokenised resources, digital profiles and reputation models.

This right is aimed at limiting algorithmic discretion over digital objects, preventing non-transparent "algorithmic arbitrariness" in the management of their status, availability or functional properties, as well as ensuring legal controllability of decisions made by automated systems without direct human participation or with minimal human intervention. Thus, algorithmic justice acts as a universal information and procedural guarantee that ensures the protection of both digital entities and digital objects within the digital jurisdiction.

The delegated rights of digital entities are derivative and strictly functional in nature and arise solely on the basis of a digital certificate of authority issued by an individual or legal entity or an authorised body of digital jurisdiction in accordance with the established information and legal procedure. Within the framework of information law, such rights should be qualified as a special regime of information representation, in which a digital entity performs legally significant actions not on its own behalf, but within a clearly defined mandate recorded in a machine-readable form.

Delegated rights may cover representation of the delegator's interests in digital legal relations, initiation and execution of transactions, management of virtual assets, access to information resources, as well as the implementation of procedural actions within the digital jurisdiction. Their scope, validity period and scenario boundaries are determined by the certificate of authority and are subject to automated control and revocation in case of violation of the terms of delegation.

By their legal nature, delegated rights are close to the institution of representation, but they differ significantly from classical civil law models by an increased level of formalisation, algorithmic determinism and technical fixation. In this sense, the delegation of rights to digital entities is not only a legal, but also an information and technological mechanism that ensures the controlled participation of autonomous systems in legal circulation without loss of jurisdictional accountability and responsibility.

Simulated rights of digital subjects are experimental, auxiliary and methodological in nature and are used mainly in research, educational, pilot or regulatory-test environments such as legal and technological sandboxes. In the field of information law, they perform the function of normative modelling and approbation of future legal regimes without direct interference in the current legal order of digital jurisdiction. Such rights allow you to reproduce complex information and legal scenarios related to autonomous data processing, algorithmic control and interaction of digital subjects and objects, without the occurrence of full-fledged legal consequences.

Simulated rights do not create legally binding powers and obligations without special human or institutional ratification, which is carried out in an established procedural manner. A prerequisite for their use is a clear, public and machine-readable disclosure of the simulated nature of the relevant digital entity or object, as well as an express prohibition of the application of simulated rights in transactions, management decisions or other actions that have legally significant consequences. In this way, simulated rights act as a tool for the controlled development of digital jurisdiction, without replacing real legal regimes and without creating risks of jurisdictional disorientation.

3.1.8. Responsibilities and ethical standards of digital actors.

The institutionalisation of the rights of digital subjects and digital objects within digital jurisdiction inevitably requires a symmetrical consolidation of the system of duties and ethical standards, without which the legal regime of digital environments acquires normative asymmetry. From the standpoint of information law, the obligations of digital subjects should be considered not as derivatives of "moral responsibility", but as elements of the regime of lawful circulation, processing and use of information that ensure the stability, predictability and security of digital jurisdiction.

The basic obligation of digital entities is the obligation to act within the legal order of digital jurisdiction, which in the field of information law should be understood as an imperative to comply with the established legal regimes for the processing, use and transformation of information. The content of this obligation includes not only formal compliance with the normatively defined scenario boundaries and conditions for delegation of authority, but also the obligation of algorithmic loyalty to legal prescriptions that regulate acceptable ways of decision-making in the digital environment.

In the information and legal sense, this obligation means the prohibition of the autonomous exit of the digital entity beyond the permitted functions, unauthorised modification of data processing modes, unauthorised change of access parameters to information resources, as well as any uncontrolled or non-transparent impact on digital objects or other participants in digital legal relations. Violation of this obligation entails the occurrence of special regimes of legal liability within the digital jurisdiction and can be qualified as an information and legal offence regardless of the degree of autonomy of the digital entity.

The second key duty of digital entities is the obligation of transparency of legal and functional status, which in the field of information law should be qualified as an imperative to ensure the openness, reliability and relevance of legally significant information necessary for the proper identification of a digital entity within the digital

jurisdiction. It is not about general information openness, but about the mandatory disclosure of exactly the information that is important for the legal regime of data processing, the attributability of algorithmic actions and the determination of the limits of responsibility.

The content of this obligation includes systematic and machine-readable information about the level of autonomy of the digital entity, the presence, scope and duration of delegated powers, the use of algorithmic or automated decision-making mechanisms, as well as the simulative, experimental or research mode of its functioning. In this sense, transparency is an element of information and legal compliance and serves as a necessary condition for the legitimate participation of a digital entity in digital legal relations.

In view of the above, transparency appears as a basic information and legal guarantee to prevent manipulation of digital identity, hidden or disguised automation, substitution of the status of a digital entity or misleading other participants in digital jurisdiction. Failure to comply with this obligation creates grounds for the application of special legal response measures, in particular, restriction of legal status, cancellation of delegated authority or prosecution within digital jurisdiction.

A separate block of responsibilities within the digital jurisdiction concerns digital objects, in particular virtual assets, data, tokenised resources, digital profiles and other information entities that have independent legal significance. In this case, it is not about the "obligations of the object" in the classical sense, but about a set of information and legal obligations of subjects to ensure the proper legal regime of digital objects as objects of law.

Such a regime includes the obligation to ensure the integrity, authenticity and relevance of data, to prevent unauthorised modification or destruction of digital objects, to comply with the established rules of access, use and alienation, as well as the obligation to maintain the full traceability of transactions with digital objects. In the field of information law, these requirements are aimed at guaranteeing evidence, legal certainty and accountability of the circulation of digital objects and are a necessary condition for their lawful participation in digital legal relations.

Ethical standards within digital jurisdiction should be considered as a normatively integrated element of information law, and not as purely declarative principles. In this context, the Code of Digital Ethics serves as a framework regulator that establishes minimum requirements for the permissible behaviour of digital entities and for algorithmic influence on digital objects. Of particular importance are the principles of non-discrimination, proportionality of algorithmic intervention and the priority of human ratification in marginal and conflict scenarios.

For simulacra and experimental digital agents within a digital jurisdiction, a special ethical and legal obligation is established for full, unambiguous and permanent disclosure of their simulative or experimental nature. In the field of information law, this obligation should be understood as an imperative to ensure information transparency regarding the ontological status of a digital agent in order to prevent erroneous identification of simulacra with full-fledged digital subjects or, moreover, with individuals or legal entities.

The content of this obligation includes the requirement of explicit marking of simulated status in digital jurisdiction registers, user interfaces and machine-readable

metadata, as well as the explicit prohibition of any form of usurpation of the digital identity of natural or legal persons, including the imitation of legal status, authority, reputational characteristics or history of lawful behaviour. Such actions are considered not only as a violation of ethical standards, but as an independent information and legal offence.

Violation of the obligation to disclose the simulative nature or prohibit the usurpation of digital identity qualifies as an informational and legal tort act that undermines trust in digital jurisdiction, distorts the mechanisms of identification and attribution of actions, and creates risks of systemic disorientation of participants in digital legal relations. In such cases, special legal response regimes may be applied, including the immediate restriction or cancellation of the legal status of the digital agent, the blocking of access to digital objects, and the initiation of legal liability procedures in accordance with the rules of information law.

Thus, the system of duties and ethical standards of digital subjects and digital objects forms the necessary regulatory counterweight to the expansion of digital rights and autonomy. It ensures the legal manageability of digital environments and creates a direct transition to the next analytical block — the problems of legal responsibility, algorithmic guilt and mechanisms of techno-guardianship within digital jurisdiction.

3.1.9. Varieties of digital subjects.

The transformation of social relations in the Metaverse environment, which is formed on the basis of convergent digital technologies, objectively necessitates a deep doctrinal rethinking of the range of subjects of information law and the mechanisms of their legal recognition. Within such an environment, not only the digitalisation of already known social practices takes place, but also the formation of fundamentally new information legal relations, in which the carriers of legally significant behaviour are intangible, algorithmic or hybrid entities that do not fit into the traditional categories of the subject of law.

The classical model of legal personality, built around the dichotomy of an individual and a legal entity, turns out to be methodologically insufficient to explain and normatively order legal relations involving avatars, digital personalities, simulacra, autonomous algorithmic agents, as well as decentralised organisational structures such as DAOs. From the standpoint of information law, the problem lies not only in the lack of appropriate definitions, but also in the lack of tools for attributing actions, responsibilities and legal consequences in an environment where subjectivity is increasingly becoming functional rather than anthropological.

In this context, the Metaverse appears as a special object and at the same time a space of information and legal regulation, within which the subject is defined not by the fact of biological existence or organisational and legal form, but by the ability to participate in information processes, generate a digital footprint, influence the rights and interests of other participants and be integrated into the system of digital jurisdiction. This is what allows us to talk about the transition from the personalist model of the subject of law to the functional-informational model of digital legal personality, which requires normative specification within the framework of digital and information legislation. Accordingly, there is a need for a new harmonised legal concept of digital entities of the

Metaverse as participants in information legal relations of a new type, the definition of their functional purpose, role and place in the system of digital jurisdiction, as well as a comprehensive characterisation of their legal personality from the standpoint of information law.

3.1.9.1. Avatars as interface subjects of the Metaverse.

In the context of information law, it is advisable to define an avatar not only as a visual-spatial or sensory-interactive representation of a physical one (Kostenko, 2020; General Data Protection Regulation, 2016)[1, 2], or a non-physical being (including artificial intelligence agents), but as a special technical and legal tool for the subject's participation in information legal relations of the Metaverse. The avatar acts as a formalised shell of digital presence, through which access to information resources, services, digital assets, communication channels and algorithmic procedures is carried out.

From the standpoint of information law, the avatar is not an independent carrier of primary legal personality, but acquires the status of a derivative (delegated) subject, through which the information rights, freedoms and obligations of an individual or legal entity are realised (Lucchetti, 2017)[3]. It is through the avatar that the identification of the subject in the digital environment is carried out, access to information systems is authenticated, as well as the fixation and accumulation of a digital trace that is of legal importance for proving, attributing actions and establishing responsibility (Figure 38).

In this sense, the avatar fulfils the key function of an information and legal intermediary between the real subject and the Metaverse environment. Its legal nature is functional: the avatar does not "replace" the person, but ensures their inclusion in the digital jurisdiction through a technically formalised presence (Seldon News, n.d.; BitExpert, 2022)[4,5]. Accordingly, any actions performed by an avatar are, as a general rule, legally attributable to the entity that exercises control over the corresponding digital identity or has delegated authority (Davis et al., 2009)[6].

1 Kostenko, O. (2020). Identification data management: Legal regulation and classification. *Scientific Journal of Polonia University, 43*(6), 198–204. https://doi.org/10.23856/4325

2 egulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union, L119*, 1–88. http://data.europa.eu/eli/reg/2016/679/oj

3 Lucchetti, S. (2017). *Why artificial intelligence will need a legal personality*. https://lawcrossborder.com/2017/05/22/why-robots-need-a-legal-personality/

4 Seldon News. (n.d.). *Full analytics in real time.* https://news.myseldon.com/ru/news/index/264050730

5 BitExpert. (2022). *Tencent unveiled a platform for creating digital people*. https://bitexpert.io/news/tencent-predstavila-platformu-dlya-sozdaniya-tsifrovyh-lyudej/

6 Davis, A., Murphy, J., Owens, D., Khazanchi, D., & Zigurs, I. (2009). Avatars, people, and virtual worlds: Foundations for research in metaverses. *Journal of the Association for Information Systems, 10*(1). https://doi.org/10.17705/1JAIS.00183.

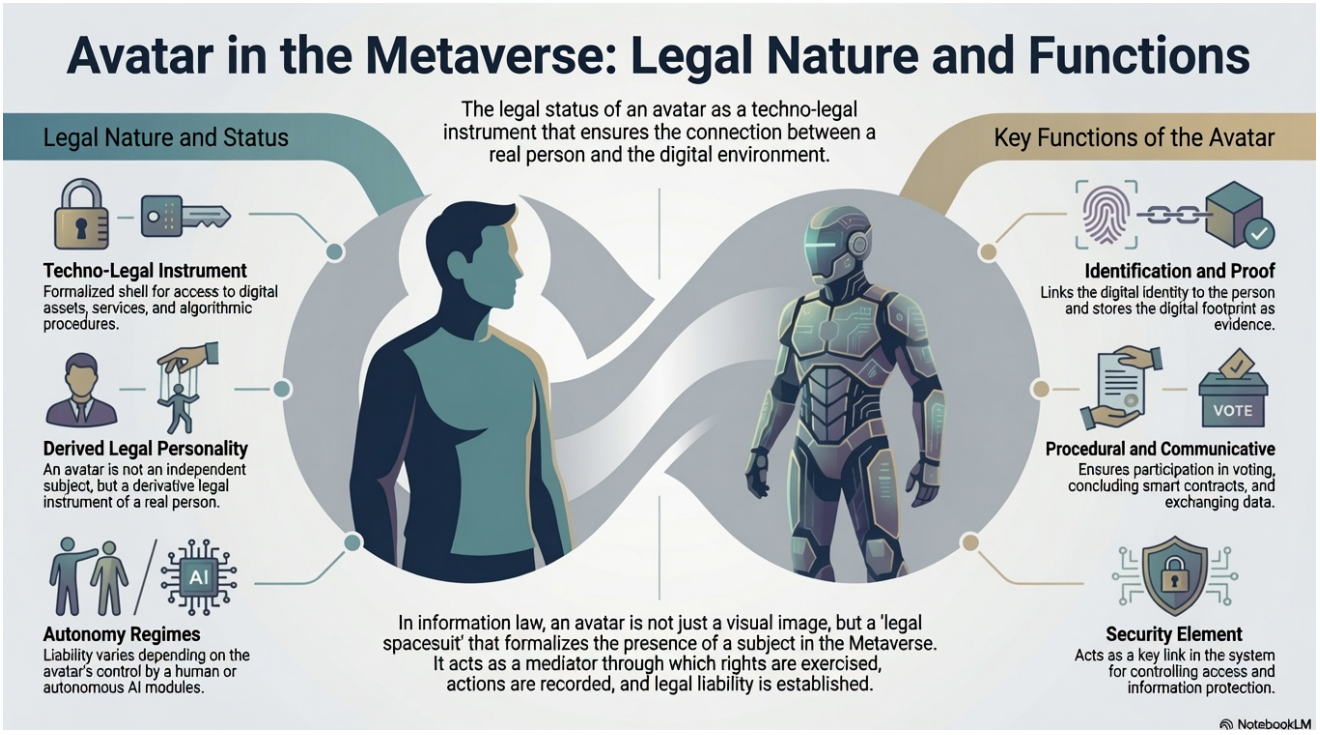


Figure 38. Metaverse: Avatars.

With this in mind, an avatar in the information law system performs the following main functions:

identification — provides a connection between a digital action and a specific subject of law (Kostenko, 2020b)[1];

communication — realises the right to information interaction, data exchange and participation in digital processes (Chin, 2007) [2];

evidentiary — forms and stores a digital footprint as a potential object of proof within a digital jurisdiction (Bryson et al., 2017; (Noval, 2023)[3,4];

procedural — ensures the participation of the subject in digital procedures (voting, concluding smart contracts, access to services) (Cheng, 2006) [5];

security — acts as an element of the information security and access control system (Cheng, 2006; Cheong, 2022; Mulyono & Sihombing, 2023) [6,7,8].

In this context, it is advisable to interpret the philosophical and legal dimension of the avatar as a kind of "legal spacesuit" of digital action, which not only visualises the

1 Kostenko, O. V. (2020b). Identification data management: Legal regulation and classification. *Scientific Journal of Polonia University, 43*(6), 198–204. https://doi.org/10.23856/4325

2 Vrontis, D., El Nemar, S., Ouwaida, A., & Sakka, G. (2023). Virtual reality and the metaverse: A systematic review and future research agenda. *Journal of Business Research, 164,* Article 113978. https://doi.org/10.1016/j.jbusres.2023.113978

3 Chin, B. (2007). Regulating your second life: Defamation in virtual worlds. *Brooklyn Law Review, 72*(4), 1303–1349.

4 Bryson, J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law, 25*, 273–291. https://doi.org/10.1007/s10506-017-9214-z

5 Noval, S. M. R. (2023). Metaverse, avatar and illusion of lawless world: Rethinking boundaries in virtual world. In *Proceedings of the International Seminar on Border Region (INTSOB 2023)*. (pp. 312–325). Atlantis Press https://doi.org/10.2991/978-2-38476-208-8_29

6 Cheng, T. S. L. (2006). A brave new world for intellectual property rights. *Journal of Law, Information and Science, 17*, 10. http://www5.austlii.edu.au/au/journals/JlLawInfoSci/2006/2.html

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

8 Mulyono, A., & Sihombing, E. (2023). The phenomenon of avatars as subjects of law in the metaverse. *Jurnal Ilmiah Penegakan Hukum*. https://doi.org/10.31289/jiph.v10i1.9091

presence, but also institutionalises it in a form suitable for legal regulation. It is through the avatar that information law gets the opportunity to work with intangible forms of participation, translating them into the plane of normatively defined information relations.

At the same time, it should be emphasised that the level of autonomy of the avatar is of fundamental importance for determining the scope of rights and responsibilities (Dwivedi et al., 2023).[1] An avatar that functions exclusively under the direct control of a person is in full delegation mode, while avatars integrated with algorithmic agents or AI modules can perform semi-autonomous actions, which requires a special information and legal regime of control, auditing and limitation of powers (Zelenyanszki et al. , 2023)[2].

Thus, within the framework of information law, the avatar appears not as a technical detail of the virtual environment, but as an independently significant element of the legal ontology of the Metaverse, through which the attribution of actions is implemented, information security is ensured, and the basis for digital jurisdiction is formed.

At the same time, an avatar is a complex digital object that combines the features of the result of intellectual activity and information structure with a multiple legal regime. From the standpoint of information law, it is advisable to consider an avatar primarily as an intangible digital good related to the identification of a person, the processing of personal and behavioural data and the implementation of personal non-property rights, and its legal protection can be carried out within the framework of copyright and a special sui generis regime. If the avatar is created using digital tools, then the copyright belongs to the respective developers. An avatar is an intangible good, which can include such virtual objects as: a game character tied to a specific user; a person's profile on a social network; a computer copy of a person with unique identification features, originality and objective form. It has the following characteristics: the presence of a digital objective form, which makes it possible to perceive the avatar in the digital environment, originality, uniqueness, and the presence of legal access to the use of the avatar. Legal protection of an avatar within the framework of copyright can be carried out under two legal regimes: copyright protection; and the institute of law of a special kind (sui generis) (Kroitor, 2023)[3].

3.1.9.2. Digital personalities as carriers of digital identity.

Within the framework of information law, digital personality should be considered not as an auxiliary or derivative characteristic of the subject, but as an independent legal construct that provides the opportunity to participate in information legal relations outside the physical presence. In the doctrinal dimension, digital identity is defined as a legally recognised set of identification attributes, information profiles, behavioural patterns, interaction history, and legal status that collectively allow the attribution of actions, decisions, and legal consequences to a specific entity in the Metaverse digital environment.

1 Dwivedi, Y. K., Kshetri, N., & Hughes, L. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-023-10400-x

2 Zelenyanszki, D., Hóu, Z., Biswas, K., & Muthukkumarasamy, V. (2023). A privacy awareness framework for NFT avatars in the metaverse. In *2023 International Conference on Computing, Networking and Communications (ICNC)* (pp. 431–435). https://doi.org/10.1109/ICNC57223.2023.10074107

3 Kroitor, V. (2023). Avatar legal protection as an atypical copyright object. *Bulletin of Kharkiv National University of Internal Affairs*. *102*(3), 29–38. https://doi.org/10.32631/v.2023.3.03

Let's apply the author's definition: Digital identity within the framework of information law is an independent legal construct and information and legal mechanism of individualisation of the subject in the digital environments of the Metaverse and digital jurisdiction, consisting of a structured array of data and metadata, designed for authentication, authorisation, legal individualisation and inclusion of the subject in digital systems, which ensures the attribution of actions, decisions and legal consequences to a specific subject in digital environment, regardless of its physical presence or spatial localisation, with the possibility of applying control, compliance, appeal, and information and legal coercion.

From the standpoint of information law, a digital person acts as a carrier of digital identity, which should be understood as a structured array of data and metadata that provides unambiguous recognition of the subject in digital systems, its authentication, authorisation and legal individualisation. Unlike the avatar, which performs a predominantly front-end function, the digital identity has normative significance as a centre for the attribution of information rights and obligations, as well as a point of legal responsibility (Figure 39).

The legal significance of the digital personality lies primarily in the possibility of separating the subject from his physical physicality and spatial localisation. It is the digital identity that allows you to ensure the continuity of the legal status of a person in multiple digital environments, platforms and spaces of the Metaverse, as well as integrate it into the system of digital jurisdiction regardless of territorial borders. In this sense, the digital identity fulfils the function of a legal "anchor" to which the actions of avatars, algorithmic agents and other tools of digital interaction are attached.

In the structure of information legal relations, the digital personality ensures the implementation of the following basic functions:

identification — the establishment of a legally significant connection between the information action and a specific subject;

attributive — attribution of the results of actions, messages, transactions and algorithmic decisions to a certain bearer of rights and obligations;

reputational — the accumulation of a history of digital behaviour, which can be taken into account when granting access, delegating authority or determining the level of trust;

compliance — ensuring compliance of the subject's actions with the requirements of digital law and order, information security standards and algorithmic transparency;

jurisdictional — inclusion of the subject in the system of digital jurisdiction with the possibility of applying control, appeal and coercion procedures.

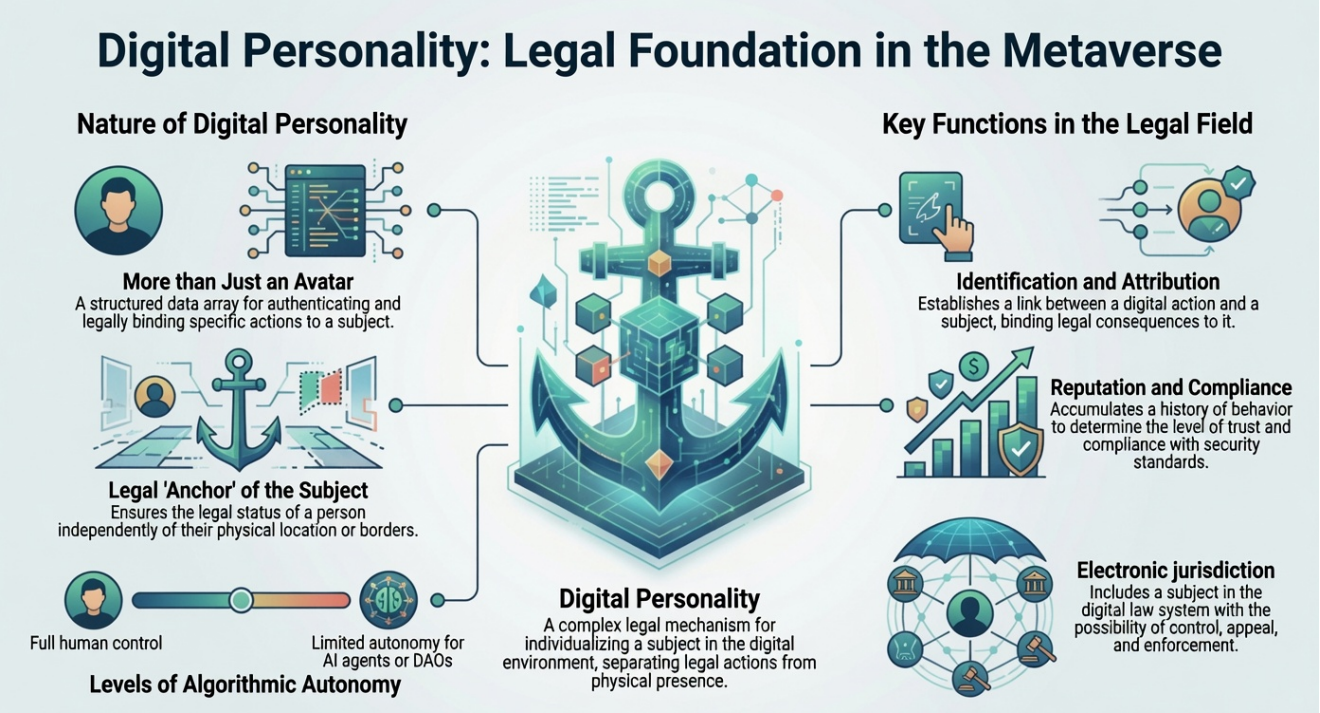


Figure 39. Metaverse: digital identity.

Depending on the degree of algorithmic autonomy and the nature of control, digital identities can have different levels of autonomy. The digital identity of an individual, as a rule, is in the mode of full or partial delegation, when all legally significant actions are finally attributed to a person. At the same time, digital personalities belonging to autonomous AI agents, DAO structures, or training language models can function in a mode of limited autonomy, in which some decisions are made without direct human intervention.

It is in this context that the digital personality acquires the characteristics of conditional informational legal personality. It is not about recognising artificial intelligence or an algorithm as a full-fledged person in the civil law sense, but about providing limited, functionally determined legal capacity within the digital legal order. Such legal capacity is derivative, reversible and controllable and can be expanded or limited depending on the level of risks, the nature of the activity and the results of the algorithmic audit.

From an information and legal point of view, the digital personality also plays a key role in ensuring information security and protecting the rights of other participants in the digital environment. It is through the institution of digital identity that it becomes possible to introduce regimes of personalised responsibility, algorithmic supervision, digital reputation, and preventive restriction of access in cases of abuse or systemic violations.

Thus, the digital personality in the legal ontology of the Metaverse appears as the central element of information legal personality, which combines identification, behavioural and jurisdictional characteristics of the subject. Its regulatory consolidation is a necessary condition for the formation of an effective system of digital jurisdiction capable of providing legal certainty, accountability and protection of rights in digital environments.

3.1.9.3. Digital humanoids and robotic agents as subjects of the Metaverse.

Digital humanoids and robotic agents encompass a set of physical or virtual technical systems of the Metaverse that are endowed with humanoid or quasi-humanoid interaction interfaces and are capable of communication, decision-making and action in the digital and, in some cases, in the physical environment. In the context of information law, such systems cannot be considered exclusively as technical means, since their functioning is directly related to information processing, influencing people's behaviour, forming information flows and creating legally significant consequences.

Let's apply the author's definition: Digital humanoids and robotic agents are physical or virtual technical systems with humanoid or quasi-humanoid interfaces of interaction, a special category of technical and social agents of increased information and legal risk, the functioning of which, on the basis of algorithmic autonomy and information processing, is capable of communication, decision-making and action in a digital or physical environment and generating legally significant consequences that digital and hybrid environments are subject to a special legal regime of digital jurisdiction, which includes mandatory identification, risk classification, algorithmic audit, techno-custody and the use of hybrid models of legal liability.

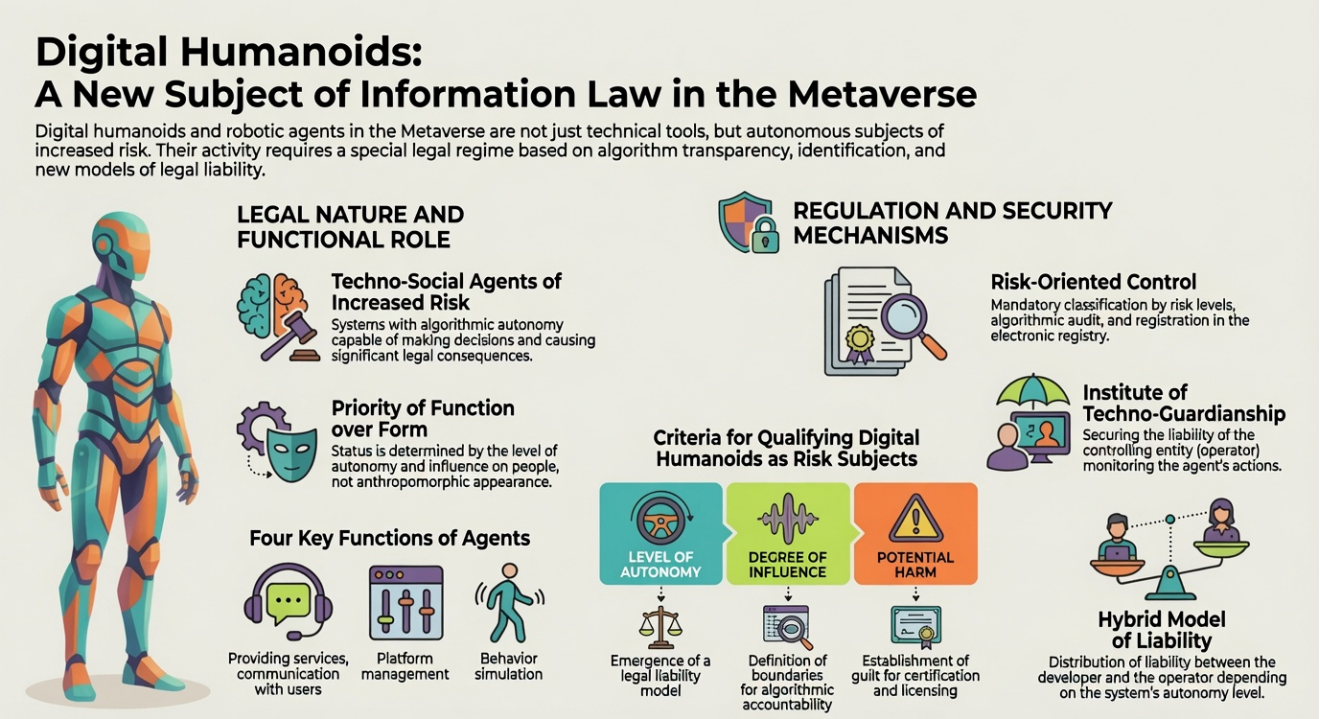


Figure 40. Metaverse: Digital Humanoids.

The legal nature of digital humanoids is determined not by their anthropomorphic characteristics, but by their functional role in information legal relations (Figure 40). Crucial: the level of autonomy of algorithms, the ability to self-learn, the intensity of information influence on other actors, as well as the potential to harm information security, human rights or public interests. It is according to these criteria that digital humanoids and robotic agents should be qualified as subjects of increased information and legal risk.

From the standpoint of information law, it is advisable to attribute digital humanoids to a special category of technical and social agents, whose activities require a special regulatory regime. Such a regime should combine elements of information security, algorithmic control, preventive regulation and enhanced legal supervision. First of all, it is about establishing mandatory requirements for the transparency of algorithms, predictability of behaviour, the possibility of auditing decisions and limiting scenarios of interaction with humans.

In the structure of information legal relations, digital humanoids can perform various functions: service (provision of information services), communication (interaction with users in virtual environments), managerial (participation in decision-making in digital platforms), as well as simulation (modelling of social or professional behaviour). Each of these functions gives rise to specific information and legal risks, in particular, the risk of manipulation, disinformation, psychological influence or substitution of human participation for algorithmic ones.

Particular attention should be paid within the framework of information law to the issues of attribution of actions of digital humanoids. As a general rule, legal responsibility for their functioning rests with individuals or legal entities who carry out the development, implementation, training or operation of the relevant systems. At the same time, in cases where a robotic agent operates in a semi-autonomous or autonomous mode, there is a need to apply distributed or hybrid liability models that combine elements of tort, administrative and informational liability.

In this context, it is expedient to introduce the institution of techno-guardianship as a special information and legal mechanism for controlling digital humanoids. Technical guardianship involves the assignment of a responsible entity (operator, curator or supervisory authority) that ensures that the behaviour of a robotic agent meets the requirements of digital law and order, monitors information influences and has the authority to limit or terminate the functioning of the system in case of violations.

In addition, digital humanoids as subjects of information legal relations should be subject to mandatory classification by levels of risk and autonomy, which should be reflected in the relevant registers of digital jurisdiction. Such a classification allows differentiating legal regimes for their use, establishing special requirements for certification, licensing and information security, as well as ensuring preventive protection of human rights in interaction with algorithmic systems.

Thus, digital humanoids and robotic agents in the legal ontology of the Metaverse appear as complex technical and informational subjects that combine elements of an object and a subject of law. Their legal regulation within the framework of information law should be based on a risk-based approach, the principles of harm prevention, algorithmic transparency and accountability, which is a prerequisite for the safe and legitimate functioning of Metaverse environments.

3.1.9.4. Artificial intelligence systems with corporate rights.

A separate, conceptually new group of digital entities in the Metaverse environment is made up of artificial intelligence systems that are involved in corporate, quasi-material or managerial relations and are endowed with a limited scope of rights functionally similar to corporate ones. First of all, we are talking about algorithmic systems integrated

into decentralised autonomous organisations (DAOs), digital asset management protocols, smart contract mechanisms, and other institutionalised forms of digital self-government (Figure 41).

Let's apply the author's definition: Artificial intelligence systems with quasi-real or quasi-corporate rights are algorithmic information systems integrated into decentralised or platform structures of digital self-government or functional digital agents, which are delegated the exercise of certain corporate-like powers — managing digital assets, executing smart contracts, participating in DAO votes, or monitoring internal rules — exclusively through algorithmic processing information and within the framework of clearly defined scenario restrictions, which, on the basis of a statutory functional mandate, are endowed with limited information and legal capacity to carry out legally significant actions in the digital environment of the Metaverse without acquiring the status of a full-fledged subject of law in the classical sense.

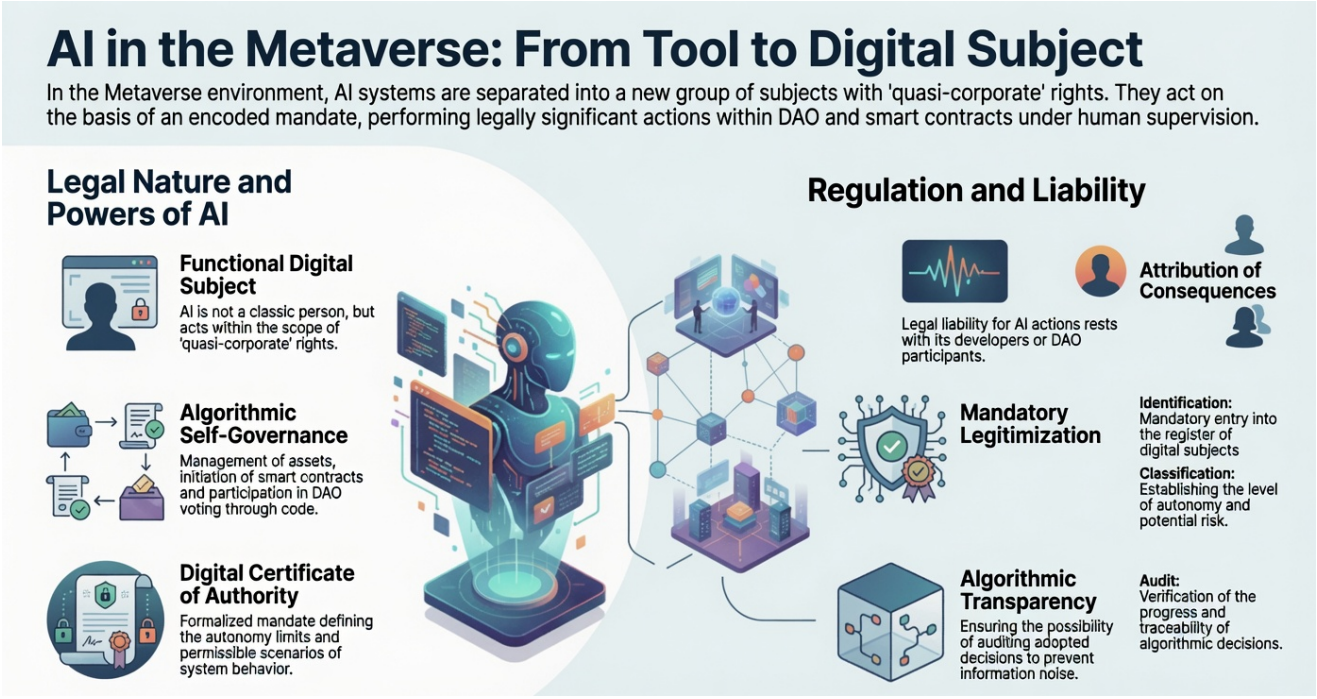


Figure 41. Metaverse: Artificial intelligence systems with quasi-tangible or quasi-corporate rights.

From the standpoint of information law, such systems cannot be qualified either as classical legal entities or as objects of law in the traditional sense. Their legal status has a conditional, functionally determined nature and is based on the principle of participation in information legal relations through the performance of certain algorithmic functions. In this sense, it is appropriate to use the category of "quasi-real" or "quasi-corporate" rights, which are not identified with property rights or corporate human rights, but provide the algorithmic system with the opportunity to perform legally significant actions in the digital environment.

The informational and legal nature of such rights lies in the fact that they are exercised exclusively through information processing, code execution and interaction with other digital subjects. The AI system can be authorised to manage tokenised assets, initiate or execute smart contracts, participate in DAO voting, allocate digital resources, or monitor compliance with the platform's internal rules. All these actions are of an

informational and legal nature, since their result is a change in the legal status of other subjects or objects in the digital environment.

At the same time, the endowment of artificial intelligence systems with such powers does not mean the recognition of their independent legal personality in the full sense. From the information and legal point of view, we are talking about a model of delegated or instrumental legal capacity, in which the algorithmic system acts as a bearer of limited rights within a clearly defined functional mandate. Such a mandate should be formalised in the form of a digital certificate of authority, which defines the scope of actions, the limits of autonomy, permissible behaviour scenarios and control mechanisms.

Of particular importance in this context is the issue of attribution of legally significant actions to artificial intelligence systems. As a general rule, the consequences of such actions should be attributed to the individuals or entities that created, implemented, or operate the relevant system, as well as to the participants of the DAO or platform that delegated authority to it. At the same time, in complex decentralised structures, it is possible to form models of collective or distributed information and legal responsibility that go beyond the classical constructions of tort or corporate law.

Within digital jurisdiction, artificial intelligence systems endowed with quasi-proprietary or corporate rights should be subject to mandatory registration, identification and classification according to the level of autonomy and risk. Such registration should ensure the transparency of algorithmic activities, the ability to audit decisions made and the effective use of information and legal control mechanisms.

Thus, artificial intelligence systems with corporate or quasi-proprietary rights in the legal ontology of the Metaverse appear as special functional subjects of information law, acting not on the basis of biological or organisational nature, but through a coded mandate of participation in digital legal relations. Their regulatory regulation requires a combination of the principles of algorithmic transparency, accountability, prevention of information harm and a clear delineation of responsibility between a person, an organisation and a code.

3.1.9.6. Artificial moral agents.

Artificial Moral Agents (AMAs) constitute a separate, normatively sensitive category of digital entities of the Metaverse, the functioning of which is directly related to the implementation of ethical norms, value restrictions and principles of harm prevention in automated decision-making processes. Within the framework of information law, it is advisable to consider AMAs not as carriers of morality in a philosophical or anthropological sense, but as specialised algorithmic systems designed to formalise, interpret and apply ethical and legal standards in the digital environment.

Let's apply the author's definition: Artificial moral agents (AMAs) are specialised algorithmic systems (algorithmic compliance tools integrated into digital platforms, DAO structures and artificial intelligence systems, etc.) designed to formalise, interpret and apply ethical and legal standards in automated information processing processes, which, within the framework of information law, function as auxiliary regulatory elements that correct the algorithmic behaviour of digital entities without acquisition of independent legal personality, without being bearers of autonomous moral or legal responsibility.

The informational and legal nature of AMAs lies in the fact that their activities are aimed at regulating information processes: collecting, processing, analysing and using data, as well as adjusting the algorithmic behaviour of other digital agents (Figure 42). AMAs can be integrated into artificial intelligence systems, Metaverse platforms, DAO structures, or digital services to prevent discriminatory decisions, manipulative information influences, human rights violations, or information harm (Incentivized Symbiosis, 2024)[1].



Figure 42. Metaverse: artificial moral agents.

From the point of view of information law, AMAs primarily perform the function of algorithmic compliance. They ensure that automated solutions comply with the requirements of digital law and order, information security, transparency, and accountability. In this aspect, AMAs can be considered as a technical analogue of internal control or a supervisory mechanism that operates in real time and is capable of blocking, modifying or signalling potentially dangerous algorithmic behaviour scenarios.

A legally significant characteristic of AMAs is their auxiliary, instrumental status. They do not act as independent bearers of rights or obligations in the full sense, but their actions may have an indirect legal effect, as they affect the admissibility, legitimacy and consequences of decisions made by other digital entities. In the case of integration of AMA into critical information systems (judicial platforms, content moderation systems, algorithmic resource management), their functioning acquires public law significance.

The AMA occupies a special place in the system of ensuring information security and human rights protection in the Metaverse digital environment. It is through the use of artificial moral agents that it becomes possible to prevent the risks of violating the right

1 *Incentivized symbiosis: A paradigm for human-agent coevolution*. (2024). https://www.researchgate.net/publication/386734217_Incentivized_Symbiosis_A_Paradigm_for_Human-Agent_Coevolution

to privacy, freedom of expression, non-discrimination and information autonomy. In this context, AMAs can be qualified as preventive information and legal protection tools aimed at reducing systemic risks associated with autonomous algorithmic decisions.

At the same time, the use of AMA raises a number of complex legal issues, including the source of ethical norms that are embedded in the algorithm, the legitimacy of their application, and responsibility for erroneous or biased decisions. From the standpoint of information law, it is fundamental that the moral rules implemented in the AMA cannot be considered as an autonomous source of law. They should be based on current legislation, generally recognised principles of law, human rights standards and approved codes of ethics.

Within a digital jurisdiction, AMA activities must be subject to mandatory certification, algorithmic audit, and legal validation procedures. Such validation should include an assessment of the compliance of embedded ethical models with the requirements of information law, an analysis of the risks of discrimination or covert influence, as well as a check of the mechanisms of explainability and the possibility of appealing the results of the AMA's work.

Thus, artificial moral agents in the legal ontology of the Metaverse appear as auxiliary, but strategically important elements of information and legal regulation, ensuring the integration of ethical principles into algorithmic processes. Their normative consolidation should take into account the priority of law over code, the principle of accountability, and the need to preserve a person as the ultimate bearer of moral and legal responsibility.

3.1.9.7. Digital (virtual) influencers.

Digital (virtual) influencers constitute a special category of digital entities operating at the intersection of information, media and consumer law, as well as the right to protect personal data and counteract manipulative information practices. We are talking about virtually constructed images — avatars or simulacra created using artificial intelligence, machine learning, and computer graphics technologies, which exert a systemic informational influence on an indefinite circle of people by producing content in the Metaverse, forming behavioural models, and influencing consumer or social decisions.

Let's apply the author's definition: Digital (virtual) influencers are virtually constructed digital images or algorithmically controlled or simulated information agents created using artificial intelligence, machine learning and computer graphics technologies, the activities of which are related to the distribution of socially significant content and give rise to information and legal consequences of information asymmetry between the content producer and its consumers and therefore are subject to special information and legal regime aimed at preventing manipulative practices, hidden advertising and violation of the principle of informed consent.

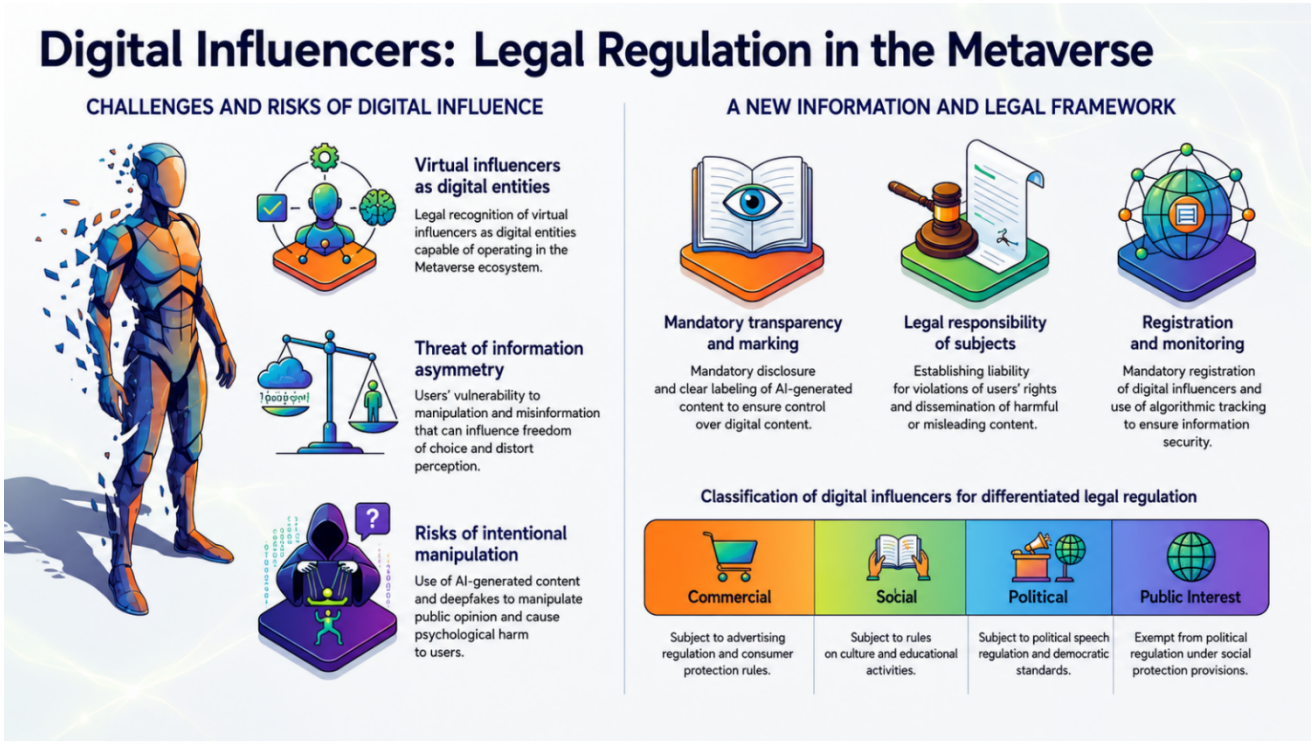


Figure 43. Metaverse: Digital Influencers.

From the standpoint of information law, the defining characteristic of a digital influencer is not its visual form or degree of anthropomorphism, but the ability to exert mass information influence and form an asymmetry of information between the content producer and its consumers. It is this ability that turns a digital influencer into a legally significant element of the information environment, whose activities can affect freedom of opinion, consumer behaviour, political preferences or social attitudes (Figure 43).

In the legal ontology of Metaverse, it is advisable to qualify digital influencers as functional subjects of information influence, whose activities are subject to a special information and legal regime. Such a regime should include mandatory requirements for transparency of the influencer's digital nature, disclosure of the fact of algorithmic or artificial origin of the content, as well as identification of the persons or organisations that control, train or fund the relevant digital image.

Of particular importance is the issue of covert manipulation and misrepresentation. The use of digital influencers without proper labelling of their artificial nature creates a risk of violating the principle of informed consent of users and can be considered a form of information abuse. In this aspect, information law should ensure a balance between freedom of expression and the need to protect a person from manipulative or unfair information influence.

With this in mind, digital influencers should be subject to the rules on liability for information content, in particular in terms of spreading misinformation, hidden advertising, discriminatory or harmful messages. Legal responsibility in such cases should not be attributed to the digital shell itself, but to the individuals or legal entities who created, administer, or use the digital influencer as an information influence tool.

From an information and legal point of view, it is advisable to distinguish between different types of digital influencers depending on the nature of their activities: commercial (marketing), social (educational or cultural), politically sensitive and

experimental. For each of these types, a differentiated legal regime should be established, taking into account the level of social risk, the scale of the audience and the potential consequences of information influence.

Within the digital jurisdiction, digital influencers must be included in the system of registration and monitoring of subjects of information influence. Such registration should provide the possibility of algorithmic and legal audit of content, tracing sources of information messages and applying preventive measures in case of systemic violations of information law and order.

Thus, digital (virtual) influencers in the Metaverse legal system appear not as neutral elements of digital culture, but as full-fledged participants in information legal relations, the activities of which require regulatory regulation. Their legal status should be based on the principles of transparency, accountability and the priority of human rights protection over commercial or algorithmic interests.

3.1.9.8. Simulacrum as a standalone digital entity without a physical original.

The simulacrum in the legal ontology of the Metaverse is one of the most complex and at the same time fundamentally new categories for information law, since it is a digital entity that does not have a direct physical, biological or legal prototype in the real world, but is able to function as a relatively autonomous participant in information processes and generate legally significant consequences in the digital environment. Unlike an avatar or a digital personality, a simulacrum does not represent a specific person or organisation, but exists as a self-sufficient information construct created and maintained algorithmically.

Let's apply the author's definition: Simulacrum is a self-sufficient algorithmic information structure that does not have a direct physical or legal prototype in the real world, i.e. it is a digital entity that operates on the basis of scenario autonomy and algorithmic logic and can acquire conditional, limited and reversible information legal personality, capable of performing legally significant information actions and generating legal consequences in the digital environment within the digital jurisdiction exclusively subject to regulatory recognition, identification and establishment of a special regime of control and responsibility.

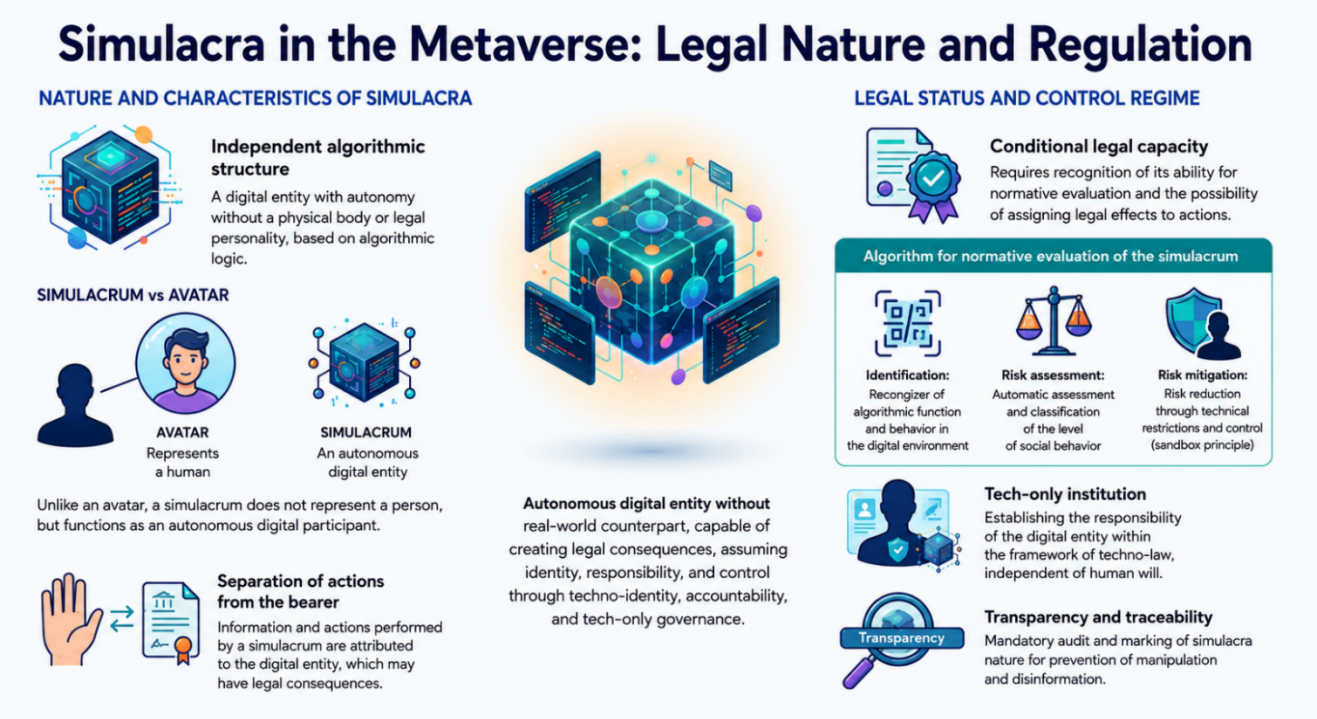


Figure 44. Metaverse: simulacra.

The legal problem of simulacra lies in the absence of a classical subject to which the actions of such a digital entity could be directly attributed within the traditional constructions of civil, administrative or criminal law (Figure 44). For the first time, information law is faced with the phenomenon when an information action is separated from a physical or organisational medium, but at the same time retains the ability to generate legal consequences. This poses a challenge to the institutions of attribution, responsibility, and jurisdiction that have historically been built around a person or entity.

In this context, the simulacrum can acquire conditional information legal personality only within the framework of digital jurisdiction and subject to a special procedure of normative recognition. Such a procedure should include, firstly, the identification of the algorithmic core of the simulacrum and the sources of its functioning; secondly, determining the level of autonomy and permissible scenarios of behaviour; thirdly, assessment of information and legal risks; fourthly, the establishment of a regime of responsibility and techno-guardianship. The legal capacity of the simulacra, in this sense, is functional, limited, derivative and reversible, that is, one that can be modified or terminated depending on the results of legal control.

Of particular importance in the information and legal regulation of simulacra is the issue of information transparency and prevention of misleading influence. Because simulacra are capable of mimicking social, professional, or communicative behaviour, their activities are associated with an increased risk of manipulation, misinformation, or usurpation of digital identity. In view of this, simulacra should be subject to mandatory labelling of their simulative nature, algorithmic audit, and a special techno-guardianship regime aimed at preventive protection of human rights and stability of the digital legal order.

In the information and legal dimension, techno-custody of simulacra performs the function of replacing the missing "human centre of will" by fixing the responsible

operator, curator or institutional supervisory entity. It is through the mechanisms of techno-care that the accountability of the simulacrum is ensured, the possibility of interfering with its functioning and the application of legal sanctions in case of violations.

Thus, the simulacrum in the legal ontology of the Metaverse appears not as a purely philosophical or cultural metaphor, but as a full-fledged object of legal regulation, which requires a rethinking of the traditional boundaries of subjectivity, responsibility and jurisdiction. Its normative understanding allows information law to adapt to the reality of digital environments, in which the source of legal consequences is not a person as such, but an autonomous information structure included in the system of digital jurisdiction.

3.2. Blockchain as an Institutional and Legal Infrastructure of the Metaverse: Ensuring Trust and Transparency

3.2.1. Briefly about blockchain

The spread of computer technologies opens up new opportunities regardless of location, previous technical equipment and user experience. According to F. Fukuyama, humanity as a whole is experiencing a comprehensive crisis of trust, a kind of epidemic of socio-spiritual AIDS of our civilisation (Lytvynov, 2019)[1]. The rapid destruction of established norms and values, the collapse of common social values correlate with a certain level of crime, the state of families and the level of trust in social institutions, the gradual leveling of the importance of the family, the growth of individualism, selfishness and the degree of distrust in state bodies, in the people around, and the destruction of generally accepted norms. It is no coincidence that the idea of a participatory economy – a socio-economic system based on the shared use of human and physical resources – has been significantly developed. This system sometimes includes (or is considered as related to it) such concepts as the network economy or shared consumption. In the report "The Sharing Economy: Accessibility Based Business Models for Peer-to-Peer Markets", prepared in 2013 by a group of analysts at PricewaterhouseCoopers for the European Commission, the sharing economy is defined as one that brings together "companies that use business models based on providing access to peer-to-peer markets" (Vigna & Casey, 2015)[2].

A blockchain (or block chain from block, chain, chain of transaction blocks) is a distributed database that stores a secure, ordered chain of records (blocks) containing a timestamp, a hash of the previous block, and transaction data submitted as a hash tree (Narayanan et al., 2016; Goldston et al., 2022)[3, 4]. Blockchain is a special type of database that is built on distributed ledger technology (DLT) and is a continuous sequential chain of blocks containing information, copies of which are stored on many different computers independently of each other. These blocks are interconnected cryptographically and chronologically, each new input block has the control data of the previous blocks. It is

1Litvinov, O. M. (2019). Essays on Postmodern Criminology.

2 Vigna, P., Casey, M. J. (2015). The age of cryptocurrency: How Bitcoin and the blockchain are challenging the global economic order. *New York: St. Martin's Press. 358*.

3 The great chain of being sure about things. (2015, October 31). The Economist. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things

4 Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton: Princeton University Press. 336 p.https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies

impossible to change a separate block of data without the consent of all participants, since it requires changing the entire array of interconnected blocks in the distributed structure. Therefore, the larger the network, the more individual records it has and the more secure it becomes (Fukuyama, 2005)[1]. Therefore, security, anonymity, and decentralisation are key factors in the popularisation and spread of blockchain, as well as a significant complication of committing destructive actions.

Based on blockchain technology together with AI and IoT, it will be quite possible to create the Internet of Values – a protocol that enjoys universal trust, performs a notarial function in relation to all transactions on the network, acts automatically transparently and in accordance with a pre-approved scenario, excludes the influence of the human factor, builds decisions based on unconditional evidence, etc.

According to the observation of the founder of the Institute for Blockchain Research, Melanie Swan, the generation of Blockchain 1.0 technology in its ideology assumed the absence of any intermediaries in the system, the next generation of Blockchain 2.0 included "smart contracts", which also did not require the participation of a third party during the execution of any transaction (Fukuyama, 2005)[2]. According to the 2016 World Electricity Survey of the international network of companies PricewaterhouseCoopers International Limited, the next generation of Blockchain 3.0 is a stage in the development of the technology, at which the concept of "smart contract" is further refined in order to create decentralised units that are governed by their own prescriptions and operate almost autonomously (The sharing economy: Accessibility-based business models for peer-to-peer markets, 2013)[3].

With the help of Blockchain 3.0 technology, it becomes possible to introduce a fully automated "smart contract" between the producer and the consumer, which will regulate and control the quality of service delivery and payments autonomously and securely. This creates significant competition for traditional business models of the financial sector, which can be completely displaced from the market segment of payment systems.

The widespread adoption of blockchain technology can radically change the functioning of other social institutions based on relations of "objectified" trust. Based on blockchain technology, it is possible to rebuild relations with the state and authorities in general, individual social institutions and entities, including the government and parliament.

Therefore, a community of people with a reliable reputation and a great potential for trust can achieve much greater success than a similar group of people who do not possess these qualities. Trust is closely related to the expectation that all participants in the relationship will perform their duties voluntarily, including without additional coercion and (or) the application of sanctions.

The preliminary agreement, which is used in blockchain technology and cannot be changed after it is agreed, is capable of protecting against arbitrariness and human error, decisions are made on the basis of predetermined evidence of the execution of the smart

1 Goldston, J., Chaffer, T. J., Martinez, G. (2022). The metaverse as the digital leviathan: A case study of Bit.Country. Journal of *Applied Business and Economics, 24(2*). https://doi.org/10.33423/jabe.v24i2.509

2 Fukuyama, F. (2005). The Great Crash. Human nature and the restoration of social order.

3 European Commission. (2013). The sharing economy: Accessibility-based business models for peer-to-peer markets. *Business Innovation Observatory.* https://www.eukn.eu/fileadmin/Lib/files/EUKN/2014/12-she-accessibility-based-business-models-for-peer-to-peer-markets_en.pdf

contract. But it is necessary to have mechanisms for implementing changes if both parties agree to them and this corresponds to their interests and legal requirements. In addition, there is an urgent need to develop a procedure for making changes to records in block chains if there was an error in entering information into the system by an careless user, or the records were subjected to illegal influence (for example, a hacker attack).

An open blockchain model in public administration can launch the process of decentralisation of society. At the state level, as well as in the field of local self-government, blockchain can most likely be introduced in the form of a closed-type model.

On the contrary, the open blockchain model is a transparent digital ledger of transactions that is reliably protected from third-party interference, including the ability to make changes to the records made. Thus, it is possible that such a model will not receive sufficient support at the level of use by state authorities or local governments.

Since the blockchain itself does not establish rules, but only describes a predetermined procedure, it does not seem likely that the regulator's functions will be transferred from the state to the community of participants in relations that are equal and endowed with the same powers. Otherwise, we will witness the birth of a new political system.

Such a self-regulating and self-managed socio-economic system based on blockchain technology, controlled by computer programs on the basis of clear and pre-approved rules, transactions in which are carried out by self-implementing digital contracts, can become either a guarantor of democracy in an open model, or a wide field for any abuses in the closed-type blockchain model.

By eliminating unnecessary intermediaries, blockchain allows for the transition to a "sharing economy", which is built on the joint creation and use of assets, as well as the ability to satisfy the interests of all parties (equal participants, P2P).

3.2.2. Blockchain in the Metaverse legal relationship system.

Blockchain allows transactions between equal participants in a single network, which consists of a network of peer nodes. Transactions of this type imply that each network participant can make a transaction directly with any other network participant without the involvement of a third-party intermediary. The elimination of such an intermediary as a third trusted party during transactions is achieved through the presence of cryptographic confirmation. The blockchain has two keys – public and private. The public key is used to view the user's transaction history, the private key is required to access the account and complete the transaction.

In order for a transaction to be successful, proof of execution is required. The concept of proof-of-work is a consensus-based mechanism that relies on the participants and is ensured by their concerted actions on the basis of a predetermined protocol. Before information about each block is stored, verification takes place using algorithms that provide each block with a unique hash code. Hash codes can be ordinary or cryptographic hash combinations. The information is checked by the majority of participants in the automatic processing mode on the basis of mathematical calculations and added to other verified blocks, increasing their total chain. As soon as the block is added to the previous one, the operation is confirmed and all participants receive a notification about it.

The innovation of this technology is that transaction information is no longer stored in a centralised database, in particular, on a specific server, but is placed (dispersed) on the devices of all network participants, which locally store it in a certain unchanged form until the next transaction is approved. Such decentralisation provides significant advantages.

The main properties of blockchain include:

1) distributed data storage registers – the concept of data storage, which is based not on a traditional centralised server, but on the formation and storage of a list of ordered records (blocks);

2) consensus algorithms;

3) cryptographic data protection mechanisms, etc.

However, the most attractive properties of blockchain in the context of a crisis of trust and persistent search for collateral, combined with the desire for simplification and the desire to get out of excessive control, is the ability to interact directly without intermediaries and control by the state, as well as institutions controlled by it, or other intermediaries. This approach is more revolutionary and fundamental than it seems at first glance, because today there is only one forced option for interaction with a legal entity as a subject of legal relations through an appeal to its representative-intermediary – an authorised person who, under the cover of a corporate veil, performs organisational and administrative or administrative functions.

Nevertheless, the elimination of the intermediary (third trusted party) does not exclude the possibility of effective use of blockchain by the state itself, for example, in the field of taxation, improvement of payment systems, electronic voting, registration of citizens, states and property, performance of administrative tasks, etc.

For reference, the first work on a cryptographically secure block chain was described in 1991 by Stuart Haber and W. Scott Stornetta in the article "How to time-stamp a digital document" (Haber & Stornetta, 1991)[1] about an information system, which states that fixed timestamps of documents cannot be changed or damaged. This technology also took some time in order to inspire a person (or group of people) known as Satoshi Nakamoto to develop and present to the general public in 2008 the main component of the cryptocurrency Bitcoin (Bitcoin) based on blockchain technology. It was thanks to the blockchain that Bitcoin confidently became the first digital currency in the common sense, in the process of which the main problem of transaction confirmation and double-spending was solved without the involvement of trusted nodes or a centralised server (Figure 45).

1 Haber, S., Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99–111.

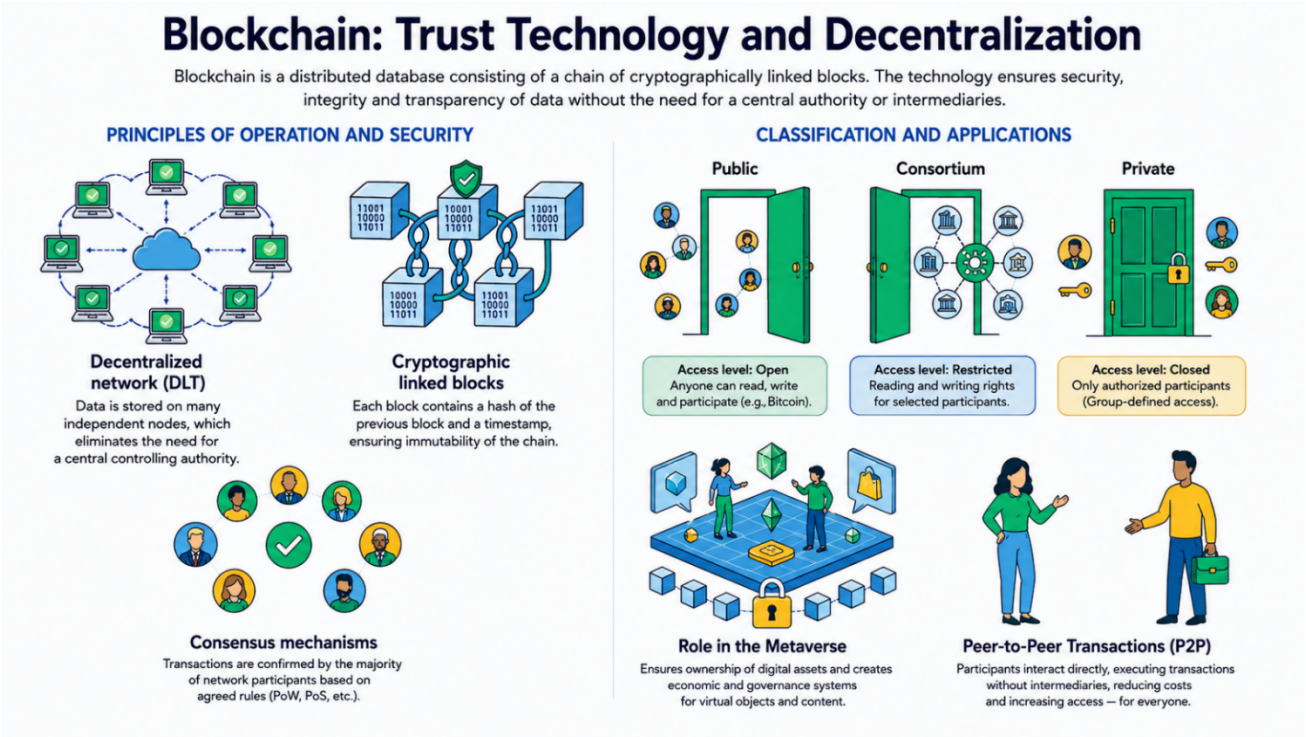


Figure 45. Metaverse: arisk architecture

The ideology and architecture of blockchain provides for different levels of access to information, which are used as criteria for classifying the varieties of the technology in question. One of these is the Canadian and British versions of the blockchain classification.

The Canadian classification provides for three types of blockchain:

a) Public blockchain – fully decentralised blockchains that are available to anyone, protected by a combination of economic rules and proof-of-work / proof-of-stake mechanisms.

b) Consortium blockchain is a partially decentralised blockchain in which the negotiation process is controlled by predetermined trust nodes.

c) Fully private blockchain is a blockchain characterised by a limited level of access to data.

The British version described in the report "Distributed Ledger Technology: beyond block chain" by Sir Mark Walport, Chief Scientific Advisor to the UK Government, is also divided into three types of blockchain:

a) Unpermissioned public ledgers – closed public ledgers.

b) Permissioned public ledgers – open public ledgers.

c) Permissioned private ledgers – open private ledgers.

Different types of blockchain can have the ability to interact with each other through the exchange of information between different platforms through the application of "blockchain transcoders" or "blockchain routers" that can work with different protocols.

One of the most popular should be considered the public blockchains Ethereum and Bitcoin. Ethereum has no ultimate beneficiary and is a public decentralised, open-source software product that is coordinated publicly and independently via the Internet. The Ethereum blockchain is open, does not require user permission, has consensus management, applies the Forkable principle (freedom to create any versions of the

blockchain), etc. (Distributed ledger technology: Beyond block chain – A report by the UK Government Chief Scientific Adviser, 2016; Wang et al., 2017)[1, 2].

The above-mentioned properties of blockchain technology have become the decisive drivers of its use in the Metaverse, which ensures data integrity and creates an electronic space of trust. For their part, cryptocurrencies are based on the blockchain and are therefore attractive for use both in the Metaverse and beyond. The Metaverse blockchain is filled with data that is created as a result of the functioning of entities and objects using blockchain platforms such as: Ethereum, Theta, Bitcoin, Binance, Smart Chain (BSC), and many others, and hash algorithms and timestamp technologies, as the main components of the blockchain data layer, can provide Metaverse users with reliability, and immutability of data.

Meanwhile, blockchain is not a static construct. The use of blockchain technology in various areas of society and human activity, including in the Metaverse, has revealed several limitations of blockchain protocols that affect their efficiency, for example, the speed of transaction processing.

3.2.3.Conceptual and terminological framework of cryptocurrencies in the Metaverse.

Since 2010, the cryptocurrency and blockchain market has grown from an experimental phenomenon to a multibillion-dollar industry. Along with the growth, numerous challenges have emerged: investor protection, anti-money laundering, tax regulation, and ensuring financial stability. States have responded with laws, bylaws, and regulatory programs (Adeniran et al., 2024)[3].

Metaverse conditions radicalise these challenges, as cryptocurrencies and related crypto assets (including NFTs) in virtual environments actually perform multiple functions simultaneously:

1) a means of exchange for the purchase of digital goods/services;

2) an investment instrument within the digital economy;

3) technological mechanism for access/identification/management of rights through smart contracts;

4) an object of civil turnover with a cross-border jurisdictional nature.

This multifunctionality creates a conflict between different regulatory models, from licensing and prudential supervision to a complete ban on cryptocurrency transactions.

Metaverse in the legal sense is not considered as a "technology", but as a set of digital environments organised by platforms, within which the following takes place:

a) circulation of digital objects (including NFTs as a form of digital objects);

b) interaction between users and service providers,

c) concluding/executing transactions (often using smart contracts);

d) making settlements/transfers, and

1 Distributed ledger technology: *Beyond block chain – A report by the UK Government Chief Scientific Adviser*. (2016). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

2 Wang, H., Cen, Y., Li, X. (2017). Blockchain router: A cross-chain communication protocol. In *Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications* (pp. 94–97). https://doi.org/10.1145/3070617.3070634

3 Adeniran, A., Alkinoon, M., Mohaisen, D. (2024). Understanding the utilization of cryptocurrency in the metaverse and security implications. In: Hà, M. H., Zhu, X., Thai, M. T. (Eds.). *Computational Data and Social Networks. CSoNet 2023*. Lecture Notes in Computer Science, vol. 14479. Singapore: Springer. https://doi.org/10.1007/978-981-97-0669-3_25

e) formation of secondary markets.

The legal specificity of the Metaverse for cryptocurrencies is that the platform economy of virtual worlds actually "embeds" financial, consumer, informational, and even evidentiary relationships into a single digital circuit: from registration/identification to settlements and disputes over rights to digital objects. This increases the importance of rules on user identification, traceability of transactions, data protection, and the legal quality of electronic evidence (including evidence, stored on the blockchain and confirmed by hash values, timestamps, electronic signatures, etc. – within the framework of the material provided) (Atrik & Zade, 2023)[1].

c) concluding/executing transactions (often using smart contracts);

d) making settlements/transfers, and

e) formation of secondary markets.

The legal specificity of the Metaverse for cryptocurrencies is that the platform economy of virtual worlds actually "embeds" financial, consumer, informational, and even evidentiary relationships into a single digital circuit: from registration/identification to settlements and disputes over rights to digital objects. This increases the importance of rules on user identification, traceability of transactions, data protection, and the legal quality of electronic evidence (including evidence, stored on the blockchain and confirmed by hash values, timestamps, electronic signatures, etc. – within the framework of the material provided) (Atrik & Zade, 2023)[2].

Today, there are at least three model approaches to definitions in the scientific community that are critically important for the Metaverse:

EU (MiCA) – focus on "uniform rules for crypto assets not covered by existing financial legislation", with requirements for transparency, disclosure, authorisation, and oversight, including stablecoins (e-money tokens/asset-referenced tokens) and service providers. Here, the key is the emphasis on a single market regime and the status of providers (authorisation/supervision).

Singapore (PSA 2019) – Definition of cryptocurrencies as "digital payment tokens": digital representations of value that are not tied to currency and are transferable. For the Metaverse, this is close to the practice of the "payment function" of cryptocurrencies.

Ukraine (Law "On Virtual Assets" 2022) – definition of a virtual asset as an intangible good that has value and is created from electronic data, while virtual assets are not a payment instrument and cannot be exchanged for goods or services.

For the Metaverse crypto economy, this norm is a conceptual point of tension, as "payments for digital goods/services" is a typical Metaverse scenario. In a technical and legal context, in the Metaverse, the same economic action (for example, payment for a digital NFT item or access to a service) in different legal systems can be qualified as: a) a payment transaction with a digital payment token; b) the circulation of a crypto asset subject to licensing by providers; c) a transaction with an intangible good that cannot be directly used as a payment instrument (Ukrainian model).

---

1 Atrik, S., & Zade, S. (2023). Metaverse crypto exchange. *International Journal of Scientific Research in Engineering and Management, 7(10*). 1-11. https://doi.org/10.55041/ijsrem26455

2 Atrik, S., & Zade, S. (2023). Metaverse crypto exchange. *International Journal of Scientific Research in Engineering and Management, 7(10*). 1-11. https://doi.org/10.55041/ijsrem26455

For the Metaverse, smart contract (as a mechanism for automating execution) and tokenisation (as a way of digitally consolidating/transferring rights) act as legal facts: they generate, change or terminate rights and obligations through technical action. Numerous studies explicitly state that the problem of a "smart contract", due to its unknown nature, does not provide a guaranteed opportunity to define it as a legitimate "contract", and therefore it cannot always be regulated by national legislation in specific moment of development (within the relevant jurisdiction/approach). This motive is important for the Metaverse: the autonomisation of the fulfilment of obligations by code creates areas of uncertainty for qualification, responsibility, and proof.

3.2.4. The Legal Nature of Transactions with Cryptocurrencies in the Metaverse.

In the Metaverse, a typical case is the purchase of a digital object (avatar items, access to an event/space, digital services) for cryptocurrency or stablecoin. Subjects: user (consumer); platform (operator/marketplace); seller/issuer of a digital object; Payment/custodial provider or exchange (if any). Object: a digital object (including NFTs) and/or a digital service; monetary equivalent in the form of a crypto asset/token. Content of rights and obligations: obligation to transfer a digital object/provide access; obligation to pay; information disclosure obligations, indemnification/consumer protection rights (depending on jurisdiction). Legal facts: blockchain transaction; acceptance of offers on the platform; execution of a smart contract.

The Ukrainian model directly fixes the restrictions: virtual assets are not a payment instrument and cannot be exchanged for goods or services. For the Metaverse, this means a collision between actual practices (crypto payments for digital goods) and the regulatory prohibition of qualifying a crypto asset as a means of payment. Technically, this creates a risk: a transaction can exist as a fact on the blockchain, but not create proper legal "payment" legitimation in the national system, making it difficult to protect consumer rights, returns, enforcement, and tax qualifications.

The issuance and circulation of NFTs in the Metaverse also has variations. Let's take a closer look at the specifics of NFT transactions for the Metaverse using the example of China.

First, the technological and regulatory attachment of NFTs to the blockchain is highlighted: "the existence of NFTs is inseparable from the blockchain," and most overseas NFT platforms are based on Ethereum; at the same time, "it is not possible to connect to the Ethereum mainnet in China," which forces platforms to develop their own blockchain or use the blockchain of Chinese companies (Cheng, 2025; Tong, 2022)[1, 2].

This immediately translates the NFT platform into a possible qualification as a blockchain information service provider with the responsibilities of filing/registering and assessing security in the "Blockchain Information Services Management Regulation" outline.

Second, the PRC explicitly describes the ban on crypto pricing/settlements in the context of NFTs: regulators "explicitly prohibit the pricing and trading of virtual

1 Chang, X. (2023). Metaverse development based on blockchain technology and NFT in China. *Academic Journal of Business & Management*, *5*(25), 158–163. https://doi.org/10.25236/ajbm.2023.052524

2 Cheng, K. (2025). NFT without crypto: China's policy, regulation and expectations of digital collectibles. *Asian Journal of Law and Economics. (4),* 5-20. https://doi.org/10.1515/ajle-2025-0049

currency," and states that companies "should not use virtual currencies such as Bitcoin, Ethereum, and Tether as pricing and settlement tools for NFT issuance transactions." This is fundamentally important for the Metaverse: even if NFTs are recognised as a digital circulating object, settlement layer (cryptocurrency) can be completely "disabled" by the right (Chang, 2023)[1].

Thirdly, it points to the regulatory emphasis on preventing the financialisation and securitisation of NFTs: "the trend of financialisation and securitisation of NFTs should be strongly restrained", it is prohibited to include financial assets (securities, insurance, loans, precious metals, etc.) in the underlying goods of NFTs, to prevent "centralised transactions... electronic matching, anonymous transactions, market makers, continuous listing transactions, standardised contract transactions, not to create trading platforms in a hidden form, and there are also requirements for real name authentication and the preservation of information and transaction records for AML purposes. For the Metaverse, this is demonstrated by the model: NFTs are allowed as cultural-digital circulation, but without turning into a "quasi-financial market" (Sun, 2024; He et al., 2022)[2,3].

Fourth, the article provides an important element of oversight in the field of intellectual property and platform liability: it is emphasised that an NFT transaction "involves the reproduction of works and the distribution of information on the Internet," and therefore the issuance/sale of NFTs without proper rights violates copyright, and the platform that charges fees must bear an increased obligation of verification. In the Metaverse, this is the practical axis of the marketplace's responsibility: it is not only a "hosting" but also a turnover operator with a potential duty of care (Guo et al., 2024; Xiao, 2023; Yu & Mao, 2024)[4, 5, 6].

In most models of regulation, it is not the "asset itself" that becomes central, but the status of the provider. In the EU, 5AMLD for the first time covered cryptocurrency exchanges and custodial wallet providers with KYC and record storage requirements. Additionally, the "travel rule" (Regulation 2023/1113) requires crypto transfers to be accompanied by information about the sender and recipient with entry into force from December 2024, it (or the related provider) is subject to identification and information requirements that limit the "pseudo-anonymity" of settlements in the Metaverse

1 Chang, X. (2023). Metaverse development based on blockchain technology and NFT in China. *Academic Journal of Business & Management*. *12*(1), 7–14 https://doi.org/10.25236/ajbm.2023.052524

2 Sun, H. (2024). "Pixel wars": *Digital collectibles trading on the Internet. Lecture Notes in Education Psychology and Public Media. 39*(1), 224–230. https://doi.org/10.54254/2753-7048/2024.bo18159

3 He, D., Liu, Z., Yang, Q., Li, L. (2022). The development of digital collection platform under responsible innovation framework: A study on China's non-fungible token (NFT) industry. Journal of Open Innovation: Technology, Market, and Complexity, *8*(4), 203. https://doi.org/10.3390/joitmc8040203

4 Guo, B., Chen, H., Li, J., , J., & Xiao, Y. (2024). Legal Regulation of Non-fungible Token Digital Collection Trading in China. *1*(4), 30–45. *Journal of Economics and Law*. https://doi.org/10.62517/jel.202414303

5 Xiao, B. (2023). Copyright law and non-fungible tokens: Experience from China*. International Journal of Law and Information Technology,* 30, 444–471. https://doi.org/10.1093/ijlit/eaad007

6 Yu, X., Mao, Y. (2024). Property rights and regulatory rules of blockchain native digital assets NFT digital collections: Starting from the first case of "Pang Hu receives vaccination". Lecture Notes in Education Psychology and Public Media, *62*(1), 115–12. https://doi.org/10.54254/2753-7048/62/20241778

(Barbereau & Bodó, 2023; Mokhniev & Muzyka-Stefanchuk, 2024; Keskitalo & Väyrynen, 2023)[1, 2,3].

Similar designs can be seen in Singapore (PSA: licences and comprehensive KYC/AML measures for exchanges, custodians, payment operators, including the "travel rule" according to MAS PS-N02) and in South Korea (VASP recognition, KYC, transaction accounting, real bank account, reporting, travel rule over ₩1 million). For the Metaverse, these modes create an architecture: the "entrance" to the crypto economy of the virtual world becomes not only technical (creating a wallet), and legally "managed" through providers (Shien, 2022; Lee et al., 2022; Takei & Shudo, 2024)[4,5,6].

3.2.5. Metaverse Crypto Economy.

European Union: MiCA, DLT Pilot, and transaction traceability. MiCA (Regulation (EU) 2023/1114) aims to establish uniform rules for crypto assets not covered by prior financial law, including transparency, disclosure, authorisation, and oversight requirements for stablecoin providers and issuers. It is important to have a transitional mechanism: entities already operating can continue to operate until July 2026, subject to the submission of a simplified application (Article 143), and the application of many rules has been postponed for 12-18 months for the adoption of acts of levels 2 and 3. For the Metaverse, the significance of MiCA is to form a "single" regime for providers through which the circulation, storage, transfer and, in fact, "legalised infrastructure" of crypto payments and the circulation of digital objects are carried out. However, in the source material, the issue of NFT coverage by MiCA mode is not explicitly detailed; Statements about this require a source in the provided material.

The DLT Pilot Regime (Regulation (EU) 2022/858, 2022)[7] creates a regulatory "sandbox" for trading and settlements using DLT, defining the types of infrastructures (marketplaces, settlement systems, combined systems) and aiming to support the tokenisation of financial instruments and protect investors by avoiding regulatory arbitrage. For the Metaverse, this is important where tokenisation goes beyond "game" items and enters the realm of tokenised financial instruments.

---

1 Barbereau, T., Bodó, B. (2023). Beyond financial regulation of crypto-asset wallet software: In search of secondary liability. Computer Law & Security Review, 49, 105829. https://doi.org/10.1016/j.clsr.2023.105829

2 Mokhniev, S., Muzyka-Stefanchuk, O. (2024). Genesis of the legal status development of virtual asset service providers in the EU. Uzhhorod National University Herald. Series: Law, *5*(3), 32–38. https://doi.org/10.24144/2307-3322.2024.85.3.5

3 Keskitalo, K., & Väyrynen, J. (2023). Fennoscandic comparison on KYC obligations of a virtual currency provider. *Journal of Money Laundering Control*. *27*(4), 738–749. https://doi.org/10.1108/jmlc-12-2022-0168

4 Shien, T. (2022). Comparative Analysis of the Payment Services Act of Japan and Singapore. *SSRN Electronic Journal*. 7(1), 1-39. https://doi.org/10.2139/ssrn.4051767

5 Lee, C., Kang, C., Choi, W., Lee, J., Cha, M., Woo, J., Hong, J. (2022). Design of blockchain-based travel rule compliance system. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1–3). https://doi.org/10.48550/arxiv.2204.13508

6 Takei, Y., Shudo, K. (2024). FATF travel rule's technical challenges and solution taxonomy. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 784–799). https://doi.org/10.1109/icbc59979.2024.10634360.

7 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU. (2022). *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2022/858/oj

AML/Travel rule: the combination of 5AMLD and "travel rule" (Regulation (EU) 2023/1113, 2023)[1] in the European model directly reduces the possibility of using the Metaverse as a medium for "diluting" the origin of funds, since crypto transfers must be accompanied by data about the sender/recipient, with a certain date of entry into force.

USA: mosaic of federal oversight, draft laws, and subnational models (taking into account Table 1). In the US, there is no single federal law regulating blockchain; there is a model of many agencies (SEC, CFTC, FinCEN, IRS, OCC, etc.) that apply existing securities, derivatives and banking laws. A list of draft laws (Responsible Financial Innovation Act, Digital Commodities Consumer Protection Act, FIT21, Digital Trading Clarity Act, etc.) designed to determine the status of digital assets and distribute powers between the SEC and CFTC, as well as the practices of individual states (for example, Wyoming – special depository institutions and DAO recognition) is indicated.

Separately, CLARITY Act (HR 3633) (Digital Asset Market Clarity Act of 2025, 2025)[2] is singled out: it aims to separate jurisdictions between the SEC and CFTC, introduce registration and reporting regimes, and stimulate innovation, aligned with FIT21 and GENIUS (stablecoins).

For the Metaverse, the American model means: the legal qualification of a crypto asset (commodity/ security/ other status) can drastically change the compliance obligations of the Metaverse platform (especially if it performs the functions of a marketplace, custodian, or operator of secondary circulation of digital assets).

A table has been formed that systematises the key regulations of the United States (federal and regional levels) and which can be directly used as an argumentative support for the analysis of the "laboratory of legal models" of the United States in the field of Web3/ Metaverse.

Table 10 demonstrates the legal "segmentation" of regulation: cryptocurrency/tokens can simultaneously fall into the orbit of securities regulations (SEC), commodity derivatives (CFTC), financial monitoring (FinCEN), tax-as-a-property (IRS), as well as state regimes (BitLicense in New York, SPDI in Wyoming, etc.). For the Metaverse, this means that the same platform can have different compliance responsibilities depending on what function it implements (NFT marketplace, custodial wallet, transfer operator, token issuer, etc.), as well as where it is "tied" jurisdictionally.

PRC: "blockchain under control" and "cryptocurrency outside the legal field". The People's Republic of China's (PRC) approach to blockchain regulation is based on a deep distinction between distributed ledger technology itself (as a neutral infrastructural basis of the digital economy) and cryptocurrencies (which are considered high-risk instruments for financial stability and social order) (Liu, 2021)[3].

- Key features of the legal regime of the PRC in the field of blockchain:
- an absolute ban on cryptocurrency activities that are not registered in the PRC. Since 2021, the People's Bank of China (PBoC) has declared all cryptocurrency

1 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849. (2023*). Official Journal of the European Union*. http://data.europa.eu/eli/reg/2023/1113/oj

2 H.R.3633 – Digital Asset Market Clarity Act of 2025. (2025). https://www.congress.gov/bill/119th-congress/house-bill/3633

3 Liu, M. (2021). Research on legal regulations of blockchain. *Advances in Social Behavior Research*. *1*(1), 10–15. https://doi.org/10.54254/asbr.2021005

transactions illegal, prohibiting the circulation, mining, exchange trading, and even the provision of crypto-related advisory services. Such a policy is justified by the need to prevent financial risks, fraud, illegal capital transfers, and energy overload due to mining (Hu, 2024) [1];

- state support for blockchain infrastructure: Along with bans on crypto assets, the Chinese government is systematically developing the Blockchain-based Service Network (BSN), a national infrastructure network for the deployment of blockchain applications, with a focus on integration with e-government, logistics, financial audit, and digital identity systems. Thus, the PRC demonstrates the model of "acceptable blockchain" under full state control;
- development of a central bank digital currency (CBDC): the digital yuan (e-CNY) is a pilot project of digital currency that is already operating in a number of cities in China, and its implementation is regulated by banking law, and the technical architecture is created taking into account the principle of "controlled anonymity" – the state is able to track all transactions as needed;
- regulation of Web3 technologies through the prism of ideological compliance: the PRC severely restricts the creation of DAOs, the circulation of NFTs, and the use of smart contracts without prior permission from regulators. The CAC (Cyberspace Administration of China), MIIT (Ministry of Industry and Information Technology) and the PBoC play a central role in this, coordinating nationwide digital initiatives through so-called "white papers" and regulatory directives.

Thus, the Chinese model is not a denial of blockchain technology, but its institutionalisation as a component of the state digital architecture. At the same time, the complete exclusion of the private crypto market from the legal field is demonstrated by the "blockchain without decentralisation" model, in which digital control is subordinated to the logic of security, ideological stability, and strategic planning (Nikitin, 2022; Shen, 2021)[2,3].

The regulation of cryptocurrencies deserves special attention as a dual approach to cryptocurrencies: on the one hand, there is a strict institutional limitation, on the other hand, there is a certain legal permissibility of ownership and private circulation.

Cryptocurrency is recognised as a "virtual commodity". Despite the ban on exchanges and mining, in court practice and explanations of regulators, cryptocurrencies, in particular bitcoin, are recognised as intangible assets that can be privately owned. This means that the possession of cryptocurrency is not illegal, and the crypto assets themselves are equated with virtual goods with economic value. This definition does not give them the status of legal tender, but allows certain transactions within the framework of civil turnover.

Although crypto exchanges are banned within the PRC, individual citizens still have the option of using foreign platforms through VPNs or foreign accounts. However, such

1 Hu, J. (2024). The regulation of cryptocurrency in China. *International Journal of Digital Law and Governance, 1*, 53–79. https://doi.org/10.2139/ssrn.4423780.

2 Nikitin, A. (2022). China blockchain internationalization opportunities: economic and technological sides. *MIR (Modernization. Innovation. Research)*, *13*(3), 459–475. https://doi.org/10.18184/2079-4665.2022.13.3.459-475

3 Shen, W. (2021). New developments on regulation of cryptocurrency in China. *Journal of Investment Compliance*. *22*(1), 53–59. https://doi.org/10.1108/JOIC-11-2020-0045

actions remain in the "grey zone" of law and can be qualified as a violation of the rules of capital circulation and cybersecurity.

The basic legal instrument of regulation to date is Order No. 3 of the Cyberspace Administration of China "Regulations on the Management of Blockchain Information Services" was reviewed and approved at a meeting of the office of the State Internet Information Administration, published and will come into force on February 15, 2019 (Cyberspace Administration of China, 2019)[1].

The Blockchain Regulation is the first comprehensive regulatory act in the PRC regulating the use of blockchain technologies. The act has the character of a ministerial-level by-law and is issued in accordance with the powers of the Cyberspace Administration of China, equated to the central executive body. The regulations consist of three main sections: the general provisions determine the object of regulation, the normative purpose and the basic principles; The main part - the obligations of the subjects - determines the requirements for blockchain service providers and users, and the final part - sanctions and establishes measures of administrative influence for violation of the norms.

The main provisions call for self-regulation of the industry, in particular, through the creation of standards that contribute to increasing the reliability of electronic evidence used in court proceedings.

The lack of unified standards for the deposit of evidence currently creates an additional burden on courts and participants in proceedings. The regulation also defines the legal obligations of providers: implementation of governance, cybersecurity and identification systems; implementing a real-name authentication policy; preliminary evaluation of new platform features; prohibition of the use of blockchain for purposes that threaten national security; mandatory registration in the file management system; the requirement to retain user data for at least six months; requirement for cooperation with state control bodies.

These provisions indicate the dominance of the concept of "digital sovereignty", which provides total control over the blockchain infrastructure at the national level. Violation of the Regulations entails quite significant administrative fines, and in some cases — criminal liability: for refusal to register users under their real name; for failure to comply with safety requirements; for lack of registration.

The regulations have the status of ministerial regulations and are mandatory for all entities working in the field of blockchain services in the PRC. Their adoption was part of China's broader strategy for information control and cyber sovereignty.

The People's Bank of China also systematically promotes the paradigm of using blockchain solutions for the real economy, especially in such areas as agriculture, logistics, energy, trade, and social insurance. Only those blockchain projects that do not involve decentralised money circulation, but are integrated into a centralised architecture controlled by the state (Bosheng Zhonghe, n.d.)[2].

---

1 Cyberspace Administration of China. (2019). *Qu kuai lian xinxi fuwu guanli guiding [Blockchain Information Service Management Regulations]*. https://www.gov.cn/gongbao/content/2019/content_5392298.htm

2 Bosheng Zhonghe. (n.d.). *Qu kuai lian Zhong-Mei xianxing falü gailan ji hegui zhanwang [A review of current laws in China and the US and a forecast of blockchain compliance]*. https://www.jialawgroup.com/single-post

Thus, the legal landscape of the PRC demonstrates a tough, but at the same time flexible approach: a total restriction of the circulation of cryptocurrency as a payment instrument and the admissibility of owning it as property, while institutionalising blockchain as a component of state digital governance. This model largely reflects the principles of "digital mercantilism" and techno-authoritarianism, within which innovations are allowed if they are subject to the state logic of control and centralised management (Bai & Zhong, 2021; Ratna, 2024)[1, 2].

The Government of the People's Republic of China pays special attention to the implementation of regulatory sandboxes, a tool that allows limited testing of innovative financial products in a controlled environment with a temporary easing of general regulatory pressure (Capkun et al., 2019)[3]. The use of sandboxes in China allows you to achieve a twofold goal: to stimulate the emergence of new financial instruments (in particular, based on blockchain architecture) and maintain regulatory control over the risks that these innovations potentially pose to the stability of the financial system. In large financial hubs — such as Shanghai, Shenzhen, Beijing — experimental zones are being implemented, within which it is allowed to test tokenised financial products, smart contracts for lending, digital wallets with biometric verification, digital identity, etc. Each project has a time limit, a limit on the number of users and transactions, as well as a strict audit system. Regulatory sandboxes are administered by the Beijing Local Financial Supervision and Administration in cooperation with the PBoC, as well as incubators at state digital technology parks. Selected blockchain startups receive support, temporary licences, and access to government testnets (for example, the internal BSN segment).

Unlike open market sandbox mechanisms operating in the US or the UK, the Chinese model excludes any uncontrolled experiments involving decentralised or anonymous value exchange mechanisms. Priority is given to projects that are integrated into the state architecture or operate in the field of fintech services without issuing their own tokens. Thus, regulatory sandboxes in China function as institutionalised zones of legal experiment that allow deregulate certain aspects of blockchain projects under the terms of full control by government agencies. In the future, this mechanism can be adapted to form a cross-border jurisdictional and technological sandbox, which is relevant for countries seeking to combine digital innovation with state sovereignty, in particular in the context of the Metaverse digital jurisdiction (Poshan et al., 2022)[4]. China's cybersecurity legislation provides general legal protection for blockchain projects, and special regulations are being developed to address new challenges in this area.

It should be noted that Hong Kong has its own regulatory system, where cryptocurrencies are recognised as property, and the market is regulated through

1 Bai, X., & Zhong, L. (2021). Legal protection of blockchain from the perspective of the cybersecurity law*: Legislation and practice of China*. (pp. 585–592). https://doi.org/10.1007/978-981-16-7993-3_45.

2 Ratna, R. (2024). Enhancing administrative penalty enforcement in market supervision through blockchain-based control and timeliness assurance. *International Journal for Research in Applied Science and Engineering Technology*. *12*(4), 1245–1251.https://doi.org/10.22214/ijraset.2024.6165

3 Capkun, S., Capkun, V., Kostiainen, K., & Wüst, K. (2019). PRCash: Fast, private and regulated transactions for digital currencies. (pp. 158–178). https://doi.org/10.1007/978-3-030-32101-7_11

4 Poshan, Y., Gong, R., & Sampat, M. (2022). Blockchain technology in China's digital economy: Balancing regulation and innovation. *In Digital Transformation and Its Role in Progressing the ICT Sector* (pp. 132–157). IGI Global. https://doi.org/10.4018/978-1-7998-7927-5.ch007

precedents and separate laws. However, the system remains complex and not always transparent to all participants (Lehenko, 2023)[1].

Switzerland: Legal Recognition of Tokenized Rights and Bankruptcy Regime - DLT Law (2021) (Swiss Federal Council, 2021)[2] amends civil and financial legislation and introduces "registered securities" – rights entered in a decentralised ledger and transferred exclusively through the ledger. For the Metaverse, this opens up the technical and legal possibility of "legally clean tokenisation" of rights and increases legal certainty regarding the custody and insolvency risks of platforms.

PSA 2019 (Payment Services Act, 2019)[3] defines cryptocurrencies as "digital payment tokens" and requires licensing of operators and comprehensive AML/KYC measures, including a "travel rule". For the Metaverse, this is a classic "payment and infrastructure" model: the legal regime is adjusted to regular transfers, settlements, and the activities of providers.

South Korea: VASP as a Financial Institution for AML Purposes (AInvest, 2025)[4]. The 2020 amendments (effective from March 25, 2021) recognise "virtual assets" and cover VASPs as subjects of the AML regime. The requirements include KYC, transaction records, a real bank account, suspicious transaction reporting, and a travel rule of more than ₩1 million. For the Metaverse, this reinforces the "tying" of the crypto economy to the banking infrastructure, which significantly affects the design of Metaverse services (especially when integrating fiat on-ramps/off-ramps).

Malta (VFA Act 2018) (Virtual Financial Assets Act, 2018):[5] mandatory whitepaper for VFA public offering, provider licensing, anti-manipulation and insider trading rules. For the Metaverse, it is relevant where a token/digital asset enters a public offering and forms a secondary market.

Gibraltar (DLT Providers Regulations 2020) (Financial Services (Distributed Ledger Technology Providers) Regulations, 2020)[6]: A 10-principle approach, including customer asset protection, information security standards, and financial crime prevention systems, with an authorisation procedure and significant fines. For the Metaverse, this could be the basis for the platform's "technology compliance."

Dubai (VA Law 2022 + VARA Rulebooks 2023) (Virtual Assets Regulatory Authority, 2023)[7]: the broad definition of virtual assets includes NFTs and AI tokens; 13 rulebooks (5 general, in AI – special); emphasis on Compliance & Risk Management and

---

1 Lehenko, V. (2023). Legal regulation of virtual assets in the Hong Kong Special Administrative Region of the PRC. *Uzhhorod National University Herald. Series: Law*. *79*(1), 227–232. https://doi.org/10.24144/2307-3322.2023.79.1.35.

2 Swiss Federal Council. (2021). *Federal Council brings DLT Act fully into force and issues ordinance.* https://www.news.admin.ch/en/nsb?id=84035

3 Payment Services Act 2019. (2019). Singapore Statutes Online. https://sso.agc.gov.sg/Act/PSA2019

4 AInvest. (2025). *South Korea's strengthening crypto AML framework and its impact on global VASP compliance and growth*. https://www.ainvest.com/news/south-korea-strengthening-crypto-aml-framework-impact-global-vasp-compliance-growth-2511

5 Virtual Financial Assets Act. (2018). Malta. https://gonzi.com.mt/investment-services-fintech-capital-markets/blockchain-icos/vfa-act/

6 Financial Services (Distributed Ledger Technology Providers) Regulations 2020. (2020). Gibraltar Financial Services Commission. https://www.fsc.gi/uploads/LRP/Financial%20Services%20(Distributed%20Ledger%20Technology%20Providers)%20Regulations%202020

7 Virtual Asset (VA) Transfer and Settlement Services Rulebook. (2023). Virtual Assets Regulatory Authority (VARA). https://amluae.com/wp-content/uploads/2023/06/Virtual-Asset-VA-Transfer-and-Settlement-Services-Rulebook-published-by-VARA-1.pdf

Technology & Information rulebooks. For the Metaverse, this is directly important: the regulator "embeds" technological and information requirements in advance into the mode of providers.

Estonia (AML Act 2022) (Money Laundering and Terrorist Financing Prevention Act, 2021): [1]the expansion of the concept of "virtual currency services" includes transfer, issuance, brokerage and DeFi platforms; FIU licence, high fees (€10,000) and increased authorised capital (€100,000/€250,000); requirements for a business plan, IT security, transaction monitoring, risk appetite, etc. For the Metaverse, this means: operators who "embed" DeFi/transfers in the virtual world, may fall under strict licensing and technological requirements.

Japan and El Salvador: Early legalisation through stock listing and the "legal tender" experiment.

Japan: mandatory registration of crypto exchange providers (PSA), prohibition of providing services without registration (Article 63-2), detailed requirements for the application and grounds for refusal (capital, organisational form, compliance systems, self-regulation). For the Metaverse, this is a hard-tolerance model through an "exchange gateway."

El Salvador: The Bitcoin Law (2021) granted Bitcoin the status of legal tender, however, on January 29, 2025, after negotiations with the IMF, the law was substantially repealed, and Bitcoin ceased to be mandatory for adoption. The conclusion here is technical and legal: the model of "forced adoption" of cryptocurrency as a legal means can create systemic (macroeconomic and regulatory) risks, and further retreat – the risk of regulatory instability.

Ukraine: legal basis without practical action and limitation of "solvency". The Law of Ukraine "On Virtual Assets" (2022) defines a virtual asset as an intangible good and expressly establishes that virtual assets are not a payment instrument and cannot be exchanged for goods or services. It introduces a classification (secured/unsecured; financial virtual assets), defines regulators (NSSMC, and for assets backed by currency values – the NBU), requires a special permit/licence for key services and establishes requirements for integrity and disclosure of ownership structure; The permit is issued for 1 year. Separately, it is recorded that the Law will enter into force after the amendments to the Tax Code, which as of July 2025 have not been adopted, so the practical application has been postponed. Ukraine has a "framework" for the regulation of providers and asset classification, but at the same time – a regulatory structure that does not allow the use of virtual assets as a payment instrument in payments for goods/services, which directly contradicts the typical function of cryptocurrency in virtual worlds. In a technical-legal sense, this requires either (a) a special model of "allowed" digital settlements in the Metaverse (a source is needed in the provided material for possible models) or (b) a clear distinction between "settlement" and "exchange of intangible goods" (a source in the provided material is needed for such qualification).

AML/CFT and "travel rule" as an anti-anonymous framework. The European 5AMLD model covers exchanges and custodial wallets with KYC and record storage,

1 Money Laundering and Terrorist Financing Prevention Act. (2021). Estonia. https://www.riigiteataja.ee/en/eli/ee/530062021006/consolide/current

and the "travel rule" requires sender/recipient data with a defined start of application. Similarly, Singapore (PSA + MAS PS-N02) and South Korea (travel rule over the threshold, reporting), Estonia (travel rule and extended AML duties).

For the Metaverse, the compliance conclusion is as follows: a platform that integrates transfers, internal marketplaces, and "embedded wallets" actually turns into a financial monitoring node. If it does not fall under the status of a provider formally, the risk of "regulatory arbitrage" increases – which is why DLT Pilot directly sets the task of avoiding arbitrage, and the Estonian model expands the VASP definition to DeFi.

The EU in MiCA provides for a block of consumer rights and information obligations (Articles 53–62 in the MiCA table), and the Ukrainian model singles out the requirements of integrity and transparency of the ownership structure of providers. Chinese material on NFTs emphasises the need to disclose information "truthfully, accurately, and completely" to protect consumer rights, right of choice, and fair trade.

Conclusion: effective consumer protection in virtual worlds is impossible without: a) regulatory binding of the responsible person (platform/issuer/seller/custodian); b) risk disclosure standards; and (c) the definition of reimbursement/refund mechanisms or equivalent procedures (within the scope of the material provided, the issue of "chargebacks" is not explicitly detailed; such an assertion requires a source in the material provided).

3.2.6. Jurisdictional Issues of Cryptocurrency Regulation in the Metaverse

The Metaverse is cross-border in nature and polycentric. These regimes demonstrate a different "degree of openness": from a detailed single market (EU) to a fragmented agency model (USA), to a total ban on transactions (China).

This leads to the basic conflict of laws problem: the same Metaverse transaction can be:

allowed and controlled (subject to the authorisation of the provider and compliance with the AML/Travel Rule) in the EU;

potentially permissible, but legally "mosaic" in status (SEC/CFTC/FinCEN/IRS) in the United States;

prohibited as a cryptocurrency transaction in China, even if blockchain technology as such is institutionalised and regulated.

The details of the conflict of laws (location of the platform/user/nodes/asset) in the provided material are not expressly spelled out; An accurate statement of doctrinal rules requires a source in the material provided. At the same time, at the level of technical and legal formulation of the issue, it is the multidirectionality of the regimes that forms the need for "compliance architecture by jurisdiction" for Metaverse platforms (geofunding, localisation of services, modularity of payment functions, etc. – specific tools need a source in the provided material).

Below is a comparative table of the technical and legal generalisation of regulatory models relevant to cryptocurrencies in the Metaverse.

Summary of Table 11 (for Metaverse). Regulatory systems converge at three "pivot points":

1) admission/licensing of providers;

2) AML/KYC and traceability (including travel rule);

3) consumer protection and market integrity (anti-manipulation).

The difference lies in the permissibility of cryptocurrencies as a payment layer: from integration and regulation (EU, Singapore) to a complete ban (PRC). For the Metaverse, this means the need for a "legally modular" architecture: the same platform must be able to operate in the mode of a licensed provider in some jurisdictions and disable crypto settlements in others (a source is needed in the provided material to describe specific tools of such modularity) (Kurt, 2022)[1].

Based on the analysed acts and models (see Tables 12–13), it is advisable to single out the following nodal problems specifically for the Metaverse:

Conflict of definitions and legal regimes: the same category of "cryptocurrency" can be a payment token (Singapore), a crypto asset under a single market regime (EU), or an intangible good that is not a payment instrument (Ukraine). For the Metaverse, this translates into a problem of transaction qualification and user legal protection.

Platform liability: in the NFT sphere (on the example of the PRC), the platform's increased responsibility for checking and preventing violations, especially in the presence of commission fees, is emphasised. In the Metaverse, similar logic applies to digital asset marketplaces and "embedded" payment services.

AML/Identity vs Privacy/Anonymity: The PRC requires real names and data retention, the EU and AI – travel rule and KYC, which for the Metaverse means a structural conflict with the "avatar" nature of digital interaction and global access.

Technology requirements as a legal obligation: VARA (Technology & Information Rulebook) and Estonian IT security and monitoring requirements show a tendency to turn technical policies into legally controllable ones.

Accordingly, the directions of improvement (in the technical and legal formulation) can be as follows:

Normative definition of "Metaverse providers" and their functions. Propose a functional approach similar to VASP logic: if a platform in the Metaverse exchanges, stores, transfers, intermediates, or issues crypto assets/tokens in the course of business, it is subject to admission/supervision requirements similar to MiCA/PSA/VARA/AML models (a specific definition formula requires legislative technique; there is no source for ready-made wording in the provided material).

Transparency and consumer protection standards for Metaverse digital marketplaces. Implement the principles of risk disclosure and consumer rights (according to MiCA's logic on transparency and consumer rights; see the description of MiCA and the consumer rights block in the starting table), with adaptation to digital goods/services in a virtual environment.

AML/Travel Rule is a differentiated compliance for the Metaverse. Taking into account the obligation to support transfers with data (travel rule) and approaches to real names (PRC), it is advisable to provide for differentiation of requirements depending on the function (transfer/custodial/marketplace), volume and risk profile in order to avoid "washing out" of innovations with excessive barriers (fundamentally, this problem is described as "high costs/compliance price" in the tables; the differentiation formula needs an additional source in the provided material).

---

1 Kurt, S. (2022). *The role of cryptocurrencies in metaverse universes*. https://www.researchgate.net/publication/366355872_METAVERSE_EVRENLERINDE_KRIPTO_PARALARIN_ROLU

NFT: banning financialisation as an optional safeguard for the Metaverse. China's approach to curbing NFT financialisation/securitisation (banning hidden marketplaces, ICO-like practices, "market makers", "anonymous transactions") can be used as a model tool for jurisdictions seeking to minimise speculative and manipulative risks in the Metaverse, but without a total ban on blockchain technology.

Ukraine: elimination of the legal vacuum and clarification of the payment regime in the digital environment. Given the delayed entry into force of the Law (due to tax changes) and the rule on the insolvency of virtual assets, the question of which actions in the Metaverse will be considered "exchange for goods/services" and which will be transactions with intangible goods in a different design requires technical and legal refinement. There is no ready-made solution in the material provided; Therefore, a source in the provided material or a separate doctrinal block of the dissertation outside of this subsection is required.

3.3. Ownership in the Metaverse: Doctrinal Approaches and Regulatory Regulation of Virtual Objects and Tokenized Assets

3.3.1. Issues of Ownership and Intellectual Property in the Metaverse

Issues of ownership and intellectual property in the Metaverse are also relevant. Today, the technical component of the Metaverse belongs to legal entities – development companies. At the same time, there are court precedents that recognise the ownership of avatars or game objects for users who have spent real financial resources on their creation and use in the gaming environment. Considering the case regarding the forced transfer of electronic game attributes, the Supreme Court of the Netherlands came to the conclusion that the virtual form of existence of the object does not matter. Intangible objects are considered property, provided that they are of value and can be controlled by a certain person. During the consideration of this case, the following arguments were put forward against the "theft" of property: virtual objects are not goods, but an "illusion" of goods consisting of bits and bytes, that is, they are data; virtual elements are information; The meaning of the game is to take objects from each other; Virtual items are and remain the property of the game's avatar, not the responder, so they could not be stolen. The court concluded that virtual objects are data, but their key feature is the possibility of individual control over them, so forcibly taking away such control from the player can be considered theft. This case was the first in Europe to become a landmark for the judicial proceedings of European countries.

One solution to the problem of enforcing rights, both for virtual world developers and users, is to distinguish between different levels of "ownership" within the Metaverse.

First level: All subjects and objects of the Metaverse are computer code that is protected by copyright law. Second level: objects in the Metaverse, like their counterparts in the physical world, are property objects. Third level: if each Metaverse object is a computer code, then copyright, intellectual and property rights are applied to it, respectively, according to the role and place of the subject in electronic legal relations, projected onto the relevant branches of law that regulate similar relations in the physical world. That is, the owner of the Metaverse of the common space can be one, the owner

of an electronic supermarket in the Metaverse can be another, the owner of an electronic product in this e-market can be a third, and the buyer is anyone (Abramovitch, n.d.)[1].

Ukrainian scholars also point to the possibility of the existence of ownership of virtual objects as incorporeal property (Nekit, 2019).[2] Scientists suggest that virtual property arises in relation to virtual objects (data) that have economic value, are objects of commodity turnover in virtual space, do not have a material shell, are unique, stable, negotiable, and are considered by owners as their own things. Such properties as uniqueness, constancy and turnover allow these objects to be included in the institution of property rights. That is, the right of virtual property arises to electronic virtual objects, which should be considered as a special type of property right, the object of which is incorporeal things (Horobets & Maisun, 2021)[3].

Property rights in the Metaverse are based on a fundamental process – the identification of the user/owner/owner of an electronic entity. Reliable electronic identification today can be ensured by using mathematical and quantum cryptography, blockchain technologies. A promising means of identification is a non-fungible token (NFT or non-fungible tokens). It is a new virtual asset that represents digital items such as images, videos, or game properties owned by users who are registered on the blockchain. The main property of non-fungible tokens (NFTs) is the guarantee that electronic assets (bitcoins, avatars, electronic goods) are owned by only one person – the user, and not by the owners of virtual systems.

3.3.2. Legal Regime of Copyright and Ownership of Virtual Objects in the Metaverse.

There is a scientific position on the expediency of applying the principle of numerus clausus in property law in relation to virtual assets (Maidanik, 2019; Nekit, 2019; It)[4,5,6] should be noted that virtual objects can be original and unique products, or they can be reliable electronic copies of real physical objects. Today, this is a promising area of technology and business development, which provides an opportunity to "clone" cities, for example, the Chinese company "51World" has created digital twins of Shanghai and Singapore. NASA successfully practices the use of electronic twins to test and monitor the performance of its spacecraft. Dassault Systèmes has created a virtual model of the human heart, which is used to develop new medical devices and analyse the safety of drugs. The Chinese company Tencent has built a digital twin of the Shanghai hospital network (Frearson, 2021)[7].

---

1 Abramovitch, S. H. *Virtual property in virtual worlds.* https://www.lexology.com/library/detail.aspx?g=5a3f3b03-a077-45d4-9981-36f713c92820

2 Nekit, K. G. (2019). Virtual Property: Concept and Essence. *Law and Society*, 2, 37–42. http://pravoisuspilstvo.org.ua/archive/2019/2_2019/part_1/8.pdf

3 Gorobets, N. O., Maysun, I. V. (2021). Virtual objects, their place in the institution of property rights. *Legal Scientific Electronic Journal*, 5, 52–54. https://doi.org/10.32782/2524-0374/2021-5/11.: http://www.lsej.org.ua/5_2021/13.pdf

4 Maidanik, R. (2019). A modernization of real law: Basic principle and directions. In *Real law: Priorities and prospects: Materials of theses of the Kyiv Legal Readings* (March 22, 2019, Kyiv) (pp. 11–19). Kyiv.

5 Nekit, K. G. (2019). Virtual property: Concept and essence. *Law and Society, 2*, 37–42. https://doi.org/10.32842/2078-3736-2019-2-7

6 Raczynski, J. (2021, October 11). *The metaverse is coming: Is the legal market prepared?* Thomson Reuters. Retrieved from https://www.thomsonreuters.com/en-us/posts/legal/legal-metaverse

7 Frearson, A. (2021, July 9). *Digital twins offer "a very powerful way of developing our cities" say experts*. Dezeen. https://www.dezeen.com/2021/07/09/digital-twins-develop-cities-digital-design-architecture/

An integral part of the overall legal issues in the Metaverse is the need for clear regulation of intellectual property rights, such as patents, copyrights, and trademarks for intangible objects (assets) in the Metaverse, as well as the taxation of virtual assets (Schneider, 2022)[1]. The problem is that modern traditional analog ownership of physical objects (assets) is limited to application to virtual objects because they are not tangible in nature. However, enforcing intellectual property rights in a virtual environment can be challenging due to difficulties in establishing ownership and verifying unauthorised use. The current legal framework needs to be carefully reviewed and adapted to the legal and regulatory challenges of the Metaverse (Kostenko & Holovko, 2023)[2].

It is important to create a clear legal framework that protects the rights of intellectual property owners and the freedom of users to create and interact with virtual objects in the Metaverse. These regulations must be fundamental in nature and affect the use of virtual objects, clarifying their legal status and ownership, which is necessary to prevent any legal problems.

3.3.3. Ownership of virtual objects.

Issues of ownership and intellectual property in the Metaverse are also relevant. Today, the technical component of the Metaverse belongs to legal entities – development companies. At the same time, there are court precedents that recognise the ownership of avatars or game objects for users who have spent real financial resources on their creation and use in the gaming environment. The Supreme Court of the Netherlands concluded that the virtual form of existence of the object does not matter. Intangible objects are considered property, provided that they are of value and can be controlled by a certain person. During the consideration of this case, the following arguments were put forward against the "theft" of property: virtual objects are not goods, but an "illusion" of goods consisting of bits and bytes, that is, they are data; virtual elements are information; The meaning of the game is to take objects from each other; Virtual items are and remain the property of the game's avatar, not the responder, so they could not be stolen. The court concluded that virtual objects are data, but their key feature is the possibility of individual control over them, so forcibly taking away such control from the player can be considered theft (The Virtual Policy Network, n.d.)[3]This case was the first in Europe to become a landmark for the judicial proceedings of European countries.

1 Schneider, J. W. S. (2022, August). *The metaverse: Patent infringement in virtual worlds*. Holland & Knight. https://www.hklaw.com/en/insights/publications/2022/08/metaverse-patent-infringement-in-virtual-worlds

2 Kostenko, O. V., & Holovko, O. M. (2023). Electronic jurisdiction of the metaverse: Challenges and risks of legal regulation of virtual reality. *Information and Law, 1*(44), 105–115. http://ippi.org.ua/kostenko-ov-golovko-om-elektronna-yurisdiktsiya-metaverse-vikliki-ta-riziki-pravovogo-regulyuvanny

3 The Virtual Policy Network. (n.d.). *RuneScape theft – Dutch Supreme Court decision*. http://www.virtualpolicy.net/runescape-theft-dutch-supreme-courtdecision.html

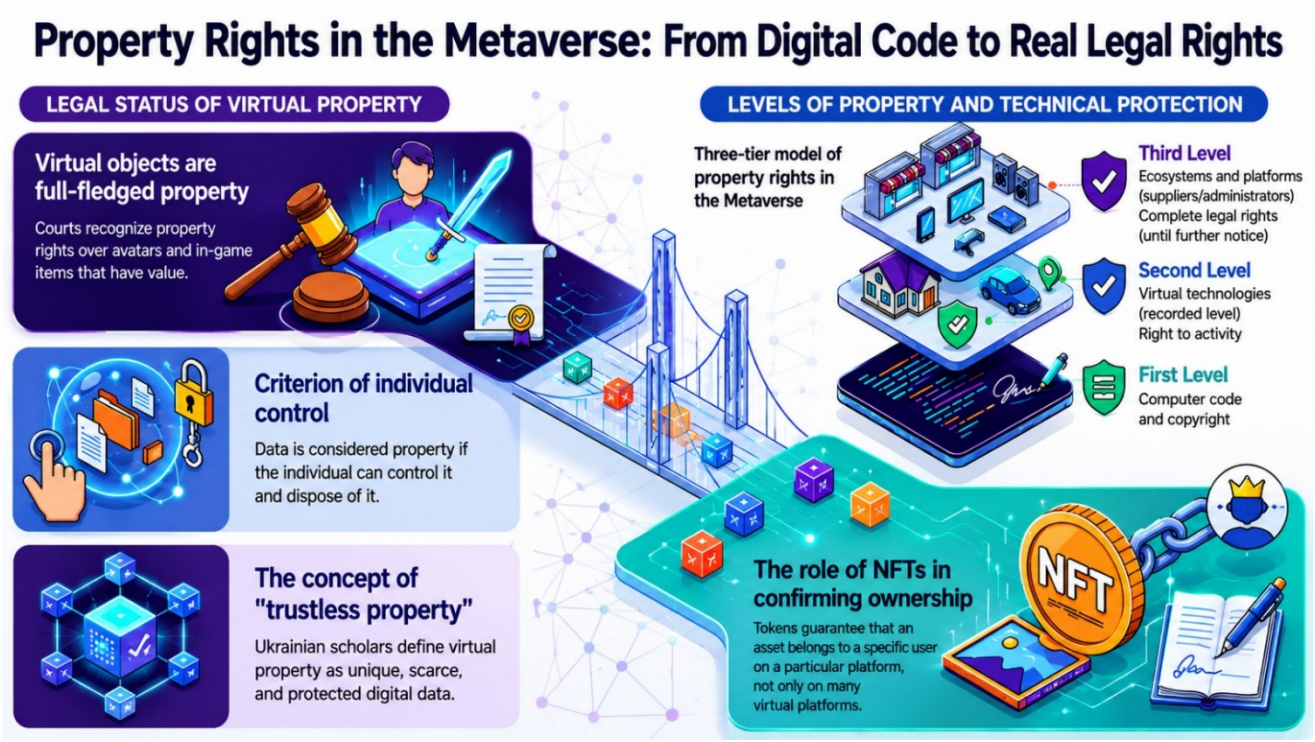


Figure 46. Metaverse and Ownership

One solution to the problem of enforcing the rights of both virtual world developers and users is to distinguish between different levels of "ownership" within the Metaverse (Figure 46).

First level: All subjects and objects of the Metaverse are computer code that is protected by copyright law. Second level: objects in the Metaverse, like their counterparts in the physical world, are property objects. Third level: if each Metaverse object is a computer code, then copyright, intellectual and property rights are applied to it, respectively, according to the role and place of the subject in electronic legal relations, projected onto the relevant branches of law that regulate similar relations in the physical world. That is, the owner of the Metaverse of the common space can be one, the owner of an electronic supermarket in the Metaverse can be another, the owner of an electronic product in this e-market can be a third, and the buyer is anyone.

Ukrainian scientists also point to the possibility of the existence of ownership of virtual objects as incorporeal property. Scientists suggest that virtual property arises in relation to virtual objects (data) that have economic value, are objects of commodity turnover in virtual space, do not have a material shell, are unique, stable, negotiable, and are considered by owners as their own things. Such properties as uniqueness, constancy and turnover allow these objects to be included in the institution of property rights. That is, the right of virtual property arises to electronic virtual objects, which should be considered as a special type of property right, the object of which is incorporeal things.

3.3.4. Copyright as a legally relevant infrastructure of "trust".

Metaverse environments (as a set of immersive digital spaces with a high proportion of UGC content, algorithmic generation, and network circulation of digital objects) radically change the architecture of copyright: a work often emerges, transforms, and is distributed in the format of protocol events (creation → modification → licensing →

micromonetisation → reuse), rather than as a one-time "act of publication". Under such conditions, copyright acquires the importance of a legally relevant trust infrastructure, since it is it that sets the normative boundaries: what is a legitimate creative result, who is the holder of the rights, what permissions are required, how authorship/legality of use is proved, and what consequences the infringement has.

Within the framework of the general matrix of the dissertation research "infrastructure - legal regimes - trust - jurisdiction", copyright plays the role of a "normative engine" for technological methods of recording and proof, modes of circulation of virtual assets, procedures for digital self-government and decentralised management on platforms, as well as mechanisms of digital jurisdiction as a tool for dispute application in the environment of interaction of many subjects and jurisdictions. In fact, without a clear legal ontology of works, rights, and licences, trust in "digital content markets" becomes fragile, and the jurisdictional capacity of platforms becomes situational.

Technical and legal characteristics of copyright processes in Web 3.0/4.0: from "protection of the work" to "registration of rights"

1) DLT/blockchain as a mechanism for recording events and evidence. Distributed ledgers (DLT) in classical technical logic are a mechanism for consistent record-keeping in a network of nodes without a single centre of trust. For copyright, legal value does not consist in "granting" a right (because the right arises from the fact of creating a work), but in recording legally relevant events:

a) the existence of a certain digital object at a specific point in time;

b) the connection between the digital object and the subject (digital identity of the author/copyright holder);

c) chain of licensing permits and transfer of rights;

d) the immutability of the audit trail, which strengthens the arguments of the party in the dispute regarding the priority, good faith and scope of lawful use.

The legally significant elements of DLT are: hashing (as a compact "imprint" of a digital object), timestamp (fixing the time of entry), block structure (sequential chain of events) and consensus (the procedure for accepting a record by the network). These elements do not automatically guarantee the "authenticity of authorship", but form the technical basis for evidence: if a party proves that a particular work/version of the work was recorded by a certain date, and the signature key/identity control was not compromised, then such a set of data gains weight in proof (especially in combination with electronic trust services and the procedure for storing electronic evidence).

2) Consensus (PoW/PoS, etc.) as a factor of responsibility and reliability of the event log. In legal analysis, it is important to avoid excessive "engineering", but it is necessary to record: different consensus mechanisms have different risks for the immutability of the journal, finality and the possibility of "rewriting" history. This directly correlates with the credibility of the registry as a source of evidence. In our opinion, in the discussion about evidence, it is advisable to move from the abstract "blockchain is reliable" to the normative question: what standard of reliability/finality is sufficient for a certain class of legal relations (deposit of a work; licensed microtransactions; collective management; recording the use of content in the Metaverse).

3) Network classifications and legal consequences of access (public/consortium/private; permissioned/unpermissioned).

Public/unpermissioned networks provide a high level of openness and verifiability of records, which is useful for public verification of priority/licence, but create complex issues of privacy and compliance with personal data regimes.

Consortium / permissioned networks (industry or institutional) are better aligned with compliance, including AML/KYC for rights and virtual asset platforms, but require a clear model of administrator responsibility and rules for accessing event logs.

Private networks can strengthen corporate rights management, but their evidentiary value in cross-border disputes will often depend on audit procedures and independent verification.

In this context, the thesis makes legal sense: the protocol access regime determines the trust regime, and therefore the ability of the digital jurisdiction to use this data as evidence and as a basis for enforcing decisions in the "protocol environment".

4) Smart contract as a legal and technological licensing tool. It is advisable to understand a smart contract in Web3/4 as a software-defined mechanism for fulfilling conditions (including payments, royalties, access restrictions) that can implement standardised "permission packages" (view/use/remix/redistribute) for digital objects. At the same time, a smart contract does not cancel the need for legal qualification: what rights are granted; whether it is consistent with imperative norms; how the conflict between the code and the text of the licence is resolved; who is responsible for code defects; what remedies are available. It is these issues that form the bridge to digital jurisdiction as a "procedure for reconciling code and law".

C**)** **"**Compliance map" technology - law - regime - risks - compliance

D**)** Copyright in the Metaverse: Architecture, Procedures, and Legal Ontology of Subjects/Objects

1) The plane of architecture. In the Metaverse, copyright is "embedded" in technical design: content exists as scenes, 3D models, textures, music, interaction scenarios, as well as "behavioural objects" (scripts, agent modules). Smart contracts and tokenisation (in the format of virtual assets) can implement licensing access modes: from simple purchase of the right to use to complex royalty schemes for secondary sales, collective rights, and the distribution of remuneration among co-authors. At the same time, it is fundamentally important to record: a virtual asset can be a carrier of an access or circulation token, but not identical to the copyright itself; it is this confusion that is the source of much of the controversy, which is confirmed by WIPO's analytics on NFTs and the "lack of clarity on what exactly is being purchased" when purchasing a token.

2) Plane of procedures. Copyright in Web3/4 is actually transformed into a set of procedures: escrow/registration (or quasi-registration via protocol), authorship verification (via digital identity), licensing (via smart contracts), usage monitoring (logging), dispute resolution (online procedures), enforcement of decisions (blocking access/reconfiguring rights in the protocol). Here, the "space of trust" means a set of technical and legal safeguards that allow relying on the protocol as an instrument of evidence and enforcement.

3) Virtual subjects and objects as elements of legal ontology. For the Metaverse, it is advisable to form a legal ontology, in which (see Appendices. Table 14):

The subjects are (a) natural persons-authors/copyright holders, (b) platforms-operators, (c) collective management organisations or DAO-like formations of digital self-government, (d) users who create derivative content;

Objects are works (including digital audiovisual and computer objects), their versions and derivative results, as well as "ancillary" objects: metadata of origin, licence tokens, event logs, reputation records.

AI generation is becoming a problematic node: different legal orders answer the question "who is the author" and whether there is a copyright for a result created without human creative activity. Ukrainian law defines an author as an individual who, through his creative activity, created a work that conceptually emphasises the anthropocentric criterion of creativity. Similarly, Indonesian law, in the WIPO Lex formula, defines an author as the person/persons who create a work on the basis of inspiration, ability, thought, imagination, etc., expressed in material form, which also gravitates towards human authorship. On the other hand, in the UK, the special construction "computer-generated works" stipulates that the author is considered to be the person who made the necessary "arrangements" to create the work, and this opens up a different model of legal attribution. The United States, on the other hand, consistently emphasises the requirement of human authorship in approaches to registration and assessment of protectability.

Thus, it can be assumed that for Metaverse regulation, the key is not the "single answer" about the author, but procedurally driven attribution: transparent disclosure of the degree of AI involvement, standards for marking origin (provenance), and spore enforcement mechanisms that allow verifying the claims of the parties.

E) Copyright Regulatory Models for Web3/4 and AI Generation: A Comparative Snippet

As an illustration of the European vector, it is advisable to mention the combination of techno-neutral copyright with specific procedural obligations for AI providers: the EU, in the AI Act, imposes an obligation on general-purpose providers to implement a policy of compliance with EU copyright law and publish a sufficiently detailed "summary" about the content used for training. At the same time, Directive 2019/790 forms a framework for text and data mining, including a "reservation of rights" mechanism for rights holders in certain cases.

A comparative legal discussion about the difference in approaches, in particular between Indonesia and the EU in the field of copyright protection from AI, is also reflected in academic publications that raise questions about the limits of the use of copyright works in model training and about the tools for protecting copyright holders.

E) Ukrainian Context: The State of the Legal Field and the Requirement of Evidence

Ukraine has an updated legislative framework for copyright: the current Law of Ukraine "On Copyright and Related Rights" dated 01.12.2022 No. 2811-IX (in the editions that were updated in 2025) consolidates the conceptual apparatus, in particular, the definition of the author, the website as a set of data, digital content, and records phenomena such as Internet piracy. This is important for the Metaverse, because "interactive access", "bringing to public knowledge" and the platform as a distribution medium are becoming typical legal facts.

At the same time, the ability of a digital jurisdiction to work with copyright disputes is impossible without general rules on electronic documents and electronic document

management, which lay the foundations for the use of electronic documents in legal relations. The Law of Ukraine "On Electronic Identification and Electronic Trust Services" is also fundamental, which sets the framework for trust services and can be used as a "bridge" between the digital identity of the copyright holder and the evidence of signed applications/licences in the protocol environment.

Separately, we would like to emphasise that the statement about the full-scale "implementation" of blockchain copyright registration at the state level or about the mandatory nature of such registers would require a direct reference to official decisions/acts. Within this subsection, no such acts are given; Therefore, any such statements without documentary confirmation would be incorrect.

E) Legal Ontology of Copyright and Jurisdictional Implications in the Metaverse

Normative and Procedural Theses as a Bridge to the Section on Electronic Jurisdiction (6–8 positions)

The thesis of the protocol as a source of evidence: in copyright disputes in the Metaverse, the evidentiary value should be determined not by the fact of "the presence of a record in the blockchain", but by the compliance of the protocol with the minimum standards: finality of the record, audit verifiability, integrity of the chain of custody, connection with the digital identity of the parties.

The thesis of due process in a protocol environment: any platform restriction of access to content/assets (freezing tokens, blocking scenes, disabling an avatar) must have procedural guarantees: notifications, the ability to file objections, neutral review, fixation of the reasons for the decision, and an appeal mechanism. In our opinion, without this, "protocol execution" turns into private coercion without legal safeguards.

Mutual recognition thesis: cross-border disputes in the Metaverse require legal interoperability profiles — standardised formats of evidence and licensing events (rights metadata, signatures, timestamps) that can be mutually recognised by platforms/arbitrations/courts under agreed rules.

The thesis of responsibility for smart contracts: legal responsibility should be distributed between (a) the initiator/copyright holder, (b) the code developer, (c) the platform operator — depending on the risk control (design/control test). This is a direct prerequisite for digital jurisdiction in determining the proper defendant and the appropriate remedy.

The thesis of "code + text" as a licence standard: to minimise disputes, licence terms in Web3/4 should exist in two agreed forms — readable (legal text) and executable (code), and conflicts between them should be resolved according to a predetermined rule (for example, text priority or code priority for technical aspects).

The thesis of algorithmic transparency of law enforcement: if the platform applies automated mechanisms for detecting violations/blocking, the necessary rules of transparency (explainability of criteria), auditability, and non-discrimination — otherwise, the platform's evidence will conflict with the right to a fair trial.

Thesis on the enforcement of decisions in the protocol: electronic jurisdiction in the Metaverse should provide for tools for the enforcement of decisions through the protocol (reconfiguration of access rights, splitting royalties, termination of illegal use), but only according to a procedure that preserves the proportionality of the sanction and the possibility of judicial/arbitration control.

The thesis of AI compliance as a provider's obligation: general-purpose providers and generation/distribution platforms must implement copyright compliance policies and disclosure of training/content origin data within the limits provided for by law; this approach is already enshrined in EU law on the obligations of GPAI providers.

In our view, a key methodological shift is to view copyright in the Metaverse as a "procedural-protocol regime," where trust is constructed not by declarations but by verifiable events, standardised evidence, and fair enforcement procedures.

3.4. Digital Legal Personality in the Metaverse: Models and Features of Implementation

3.4.1. Algorithmic legal capacity and delegated subjectivity.

The concept of algorithmic legal capacity is established, which determines the ability of a digital entity to independently or delegately perform legally significant actions. It is planned to introduce:

Limited subjectivity is a form of delegated legal personality that involves the performance of legally significant actions by a digital agent exclusively in clearly defined scenarios prescribed in a technical or legal algorithm. In this case, the agent does not make independent decisions, but only acts within pre-established conditions (for example, automatic confirmation of transactions within the allowed range, or processing user requests within a given interface). Such subjectivity does not imply legal capacity in the general civil or public legal field, but allows digital entities to be embedded in legal models such as smart contracts, digital intermediaries or service agents with pre-fixed functional logic. Its legal nature is close to the technical execution of the order, which does not create an independent legal will, but may entail consequences for the authorising party in case of failure or manipulation.

Conditional subjectivity is a model of digital subjectivity, in which the agent formally performs legal functions, but only under the condition of constant or periodic intervention of a human controller, which ensures the compliance of the agent's actions with established legal, ethical and technical standards. This form of subjectivity applies to systems capable of autonomous analytics and decision-making, but which do not pass the full legal capacity test or have a limited amount of trust.

In practice, this model is used for artificial intelligence, which generates legal opinions or recommendations (for example, in LegalTech or GovTech environments), but the final decision is approved by a human. The responsibility in such cases is shared between the algorithm developer, the system operator and the curator-reviewer, which guarantees the presence of an element of human will in the final legal act.

This allows for the gradual integration of high-tech digital entities into the legal field, maintaining regulatory control and providing real-time feedback. Examples of such systems are adaptive expert agents in forensic analytics, algorithmic advisors in administrative law, and DAO curators with manual voting or veto functions.

Simulated subjectivity is a form in which a digital subject demonstrates behaviour similar to legal activity, but does not have any recognised legal status, and therefore is not legally responsible for his actions. Such subjects are mostly elements of front-end interaction, personalised services or information agents that simulate communication,

consultation or decision-making without actually carrying them out in a legally significant form.

An example is virtual assistants, chatbots, game NPCs (non-playable characters), which create the effect of interacting with a "sentient being", but in fact only reproduce pre-programmed scenarios. In some cases, they are even capable of limited self-learning, but the result of their activities does not have the force of a legal fact.

This type of subjectivity is important in the context of information transparency: the user must have a clear message that he is interacting with the simulated subject and not with the legally responsible party. In regulation, such entities are subject to the rules on the delimitation of information and legal space, and are often regulated through transparency standards and labelling of digital products (for example, according to the provisions of the OECD AI Principles, 2019).

3.4.2.Registration, identification and coding of digital entities.

To ensure the legitimacy, traceability and legal orderliness of digital entities, it is envisaged to create a Unified Register of Digital Entities (ERCS) as part of the national digital legal infrastructure Metaverse (Figure 47). This register performs the functions of technical and legal certification, including mandatory identification, categorisation, functional marking and fixation of delegated rights.

Each digital entity receives:

A unique identifier (CID) created based on a cryptographic hash, an accounting matrix, and a set of behavioural activity parameters. The identifier is immutable, globally verified, and allows you to uniquely attribute the subject.

A functional profile displaying the range of activities allowed, autonomy level, limitations and shutdown protocols. It is based on the ISO/IEC standard 30170:2022 (Artificial Intelligence — Trustworthiness and Functional Boundaries).

Information about the creator or curator: includes the digital signature of the subject of responsibility, the developer's licensing status, organisational affiliation, and, in the case of a DAO, a public repository of source code and self-governance instructions.

Legal metadata: it is a set of attributes that describe the legal regime of the entity's activity, the jurisdiction of its registration, the possibility of revocation, the form of responsibility, as well as participation in the cross-border regimes of the Metaverse.



Figure 47. Metaverse Digital Legal Infrastructure

The EDRC should be available in API format for public, private, and international authorities to verify digital agents, ensure transactional transparency, and prevent abuse. Integration with international entity identification systems based on the principles of WIPO, EU Digital Identity Regulation (eIDAS 2.0) and IEEE 7000 is also envisaged.

Thus, the registration of a digital entity is a legal act of entering the legally regulated digital space with fixation of its essence, boundaries of authority and algorithmic responsibility.

It is envisaged to create a Unified Register of Digital Entities (ERCS) Metaverse, which fixes:

Unique identifier of the subject; This identifier is generated based on a cryptographically secure hash of data about the subject, including the algorithmic structure, the digital signature of the curator or DAO, and a verified digital creation time. CID (Cyber Identity Descriptor) performs the function of a universal digital passport of the subject, allows integration into artificial legal supervision systems, interjurisdictional tracing, and is a condition for the subject's participation in any transactions or procedural actions within the digital jurisdiction. To ensure interoperability, the identifier is tied to interoperable standards such as Decentralized Identifiers (DIDs), SSI (Self-Sovereign Identity), and EU Digital Wallet, according to eIDAS 2.0.

Coding of functionality; It is a structured description and classification of actions that a digital entity has the right or technical ability to perform. Such coding is based on unified protocols (for example, ontologies of agent behaviour, OWL/RDF classifications, or the ISO/IEC 42001 standard for AI control systems) and allows the integration of the digital entity into electronic administrative processes. Functional codes determine, in particular, the types of transactions allowed, the level of participation in the legal process (e.g. "informing", "initiating", "signing", "delegating") and the permissible limits of decision-making. This makes it possible to apply adaptive supervision modes, predict

behavioural scenarios and dynamically change the legal regime of interaction with a digital agent depending on the context ("low-risk", "audited autonomy", "human override required").

Data about the creator, owner or curator; in the case of AI agents or other digital entities, this data must contain the full legal identification of the natural or legal entity that is primarily responsible for creating, configuring, activating, and controlling the entity. Such information includes: the person's digital signature, their legal status (e.g., "individual developer," "certified AI service provider," "DAO owner"), geographic jurisdiction on which the responsibility is based, and governance policies and delegation models. In the context of DAOs or collective agents, access is granted to public documentation governing voting rules, consensus management, code updates, and responsibility sharing. This allows, in the event of a legal conflict, cyber incident or damage, to quickly identify the responsible actor in a digital law system based on the principles of attribution, traceability and procedural fairness.

Limits of responsibility and level of supervision; These parameters determine the degree of legal, operational, and reputational responsibility of the digital entity or its curator for actions that have legal consequences. The boundaries of responsibility are formalised in the form of a legal profile, which indicates:

1) whether the subject is a source of legally significant decisions;

2) what areas of legal regulation relate to his actions (for example, contract law, administrative law, public administration);

3) what form of liability is applied — personalised, distributed, collective or automated through insurance or compensation mechanisms.

The level of supervision is classified according to the scale: real-time monitoring, scheduled audit, on-demand supervision (with certain threshold actions or risks). An increase in the level of supervision can be initiated by an automatic risk indicator, an external legal request or an ethical compliance module. Systems with a high degree of autonomy are required to operate in surveillance mode with algorithmic tracking, interference protocols, and built-in self-locking mechanisms in case of detection of violations or anomalies. The level of supervision and the model of responsibility are subject to registration and approval at the time of the entity's inclusion in the ERC.

3.4.3. Normative modes of delegation of authority.

Normative delegation of authority to digital entities encompasses the legally significant transfer of part or all of the actions from a person, organisation, or other digital entity to an artificial agent or DAO in the Metaverse. Within this module, three key institutional models of delegation are defined:

Through smart contracts, legal algorithms embedded in the Metaverse blockchain infrastructure that ensure the automatic implementation of conditions that determine the delegated functions of a digital entity (for example, the right to conclude contracts, change DAO parameters, make payments, etc.). Such a mechanism guarantees the transparency, immutability and traceability of the agent's actions and allows you to encode legal obligations in a machine-readable format. Smart contracts are a mechanism in which the actions of a digital entity are rigidly defined by the conditions embedded in the program code and are automatically executed in a distributed ledger (blockchain) environment. A

smart contract comes into force after it is deployed on a platform such as Ethereum, Polkadot or Hyperledger, and its provisions become binding without the possibility of arbitrarily changing them by one of the parties. In such contracts, it is possible to encode the right of a digital entity to conclude or cancel transactions, move tokens, launch DAO voting procedures, check conditions, or change the parameters of the management object. A smart contract performs the function of not only a technical tool, but also a regulatory act that has legal effect in the digital environment.

Through digital mandates — legal tools that function similarly to classic powers of attorney, but are implemented in the form of a digital signature, activation register, and control protocols. A digital mandate can be temporarily limited, contextually conditioned, or revocable using a digital platform. It acts as a legal basis for the agent's actions in a specific administrative, procedural or contractual field. Digital mandates are formalised digital law tools that give a digital entity (such as an AI agent or DAO) a delegated right to act on behalf of another entity (person, organisation, or other agent) within well-defined legal and technological boundaries. A digital mandate is a logical and functional analogue of a classic power of attorney, but is implemented in electronic form through a digital signature, blockchain record, or verified delegation ledger. It may contain a detailed specification of powers: scope of actions, validity periods, types of decisions, acceptable risks and protocols of human intervention.

For example, a mandate may allow an agent to register intellectual property, enter into contracts, sign digital documents, or participate in administrative procedures. There are also mechanisms for the temporary suspension or automatic revocation of the mandate in cases of violation of ethical or technical restrictions. In complex cases, especially with the participation of DAOs, the mandate can take the form of multi-signature, community voting, or depend on risk indicators built into the governance algorithm.

Digital mandates are especially relevant in the context of digital jurisdiction, cross-border administrative procedures, the functioning of digital courts, as well as for the representation of the interests of minors, legal entities or other agents in virtual spaces.

Through an avatar proxy model is a model in which an entity (an individual or a legal entity) creates or controls a digital avatar that acts on its behalf in the digital environment. In this case, the proxy agent is able to represent, negotiate, participate in hearings, implement transactions, or provide services. The legal status of an avatar is formed through an act of verification, marking of conformity, and a "digital notary" system that guarantees the authenticity of the actions of such an agent. An avatar proxy model is a mechanism by which a digital avatar, as a virtual representative of a person or organisation, is empowered to act as a legal proxy in legal, administrative, or commercial digital processes. Such a model involves a high degree of personalisation: the avatar reproduces the voice, manner of speech, intellectual parameters, behavioural patterns, or even the appearance of its authoriser. In the case of integration into Metaverse or virtual platforms, such avatars can participate in negotiations, make transactions, submit applications, or carry out public communication on behalf of a real entity.

This model is implemented through avatar verification, digital authentication marking, Trusted Avatar Protocol and registration in the ERRC. In addition, the framework of the "digital notary" is used, which certifies the validity of delegated powers. The avatar model is especially relevant in the context of justice in virtual courts,

participation in virtual public hearings, representation in a digital parliament or in e-democracy institutions.

Each of these mechanisms must be technically sound, legally verifiable and ethically verified, and include conditions for suspension, revocation, appeal of the agent's actions and audit of its activities. The delegation model is necessarily fixed in the ERRC and falls under the regulatory control regimes in accordance with the level of risk, scope and degree of autonomy of the digital entity.

The legal status of the avatar depends on the level of the power of attorney, which can range from information representation to full procedural participation. High-risk scenarios require the intervention of a human moderator or ethical inspector who records the actions of the avatar in a public or commercial context. In case of violation of the boundaries of powers, there is a mechanism for revoking the digital power of attorney, blocking the avatar and initiating an administrative or civil case within the digital jurisdiction.

3.4.4.Control, audit and recall of digital subjectivity.

The functioning of digital entities in the legal field of Metaverse requires constant monitoring of compliance with delegated authority, algorithmic behaviour, and compliance with public order, technical safety, and ethical standards. In this regard, a multi-level system of supervision and institutional audit is provided.

1. Automated audit is implemented through digital agents' built-in mechanisms for monitoring, logging actions, and self-examination of functional behaviour. The audit results are stored in the form of immutable digital traces (audit trail) available for independent audits. The audit may include an assessment of compliance with given scenarios, regulatory profiles, and autonomy limits. Automated audit — this mechanism involves the constant or periodic collection and processing of data on the behaviour of a digital entity in real time or by specified triggers. The audit is carried out by built-in monitoring tools that monitor the compliance of the subject's actions with its functional profile, scenarios of permitted behaviour and the limits of delegated authority. The collected information is recorded in the form of audit trails containing timestamps, digital signatures, log files and transaction summaries, stored in decentralised or secure government registers. The results of an automated audit are used to identify risks, activate revocation or restriction mechanisms, and confirm the legitimacy of a digital agent's actions. In case of suspected violations, the audit module can automatically initiate a notification to the digital court or regulator.
2. Regular certification involves digital entities passing verification and re-assessment procedures for compliance with technical, legal, and ethical standards. Certification is carried out by authorised bodies or independent accredited structures. Certification is of particular importance for DAOs operating in the areas of public administration, finance, healthcare, or justice. It is based on ISO/IEC 42001, IEEE 7001, as well as the European AI Act. Regular certification of AI/DAO structures also involves conducting a systematic assessment of digital entities (both autonomous agents and decentralised organisations) for compliance with technical, legal, ethical, and security standards. Certification is carried out

with the help of independent accredited centres operating on the basis of international standards ISO/IEC 42001 (Management System for AI), IEEE 7001 (Transparency of Autonomous Systems), as well as the European Regulation on Artificial Intelligence (AI Act). The certification process includes: auditing the code and algorithms of the digital entity; checking documentation for compliance with the principles of transparency, non-discrimination and responsibility; AI Impact Assessment; risk analysis in the context of autonomous decision-making. Certification can be: primary (at the time of registration); regular (for example, annually or with a change in functionality); emergency (in case of violations or complaints). The presence of a certificate is a prerequisite for the admission of a digital entity to participate in high-risk transactions (financial, medical, managerial), obtaining public contracts or integration into government information systems. In addition, the certificate is recorded in the URCC and is subject to open access for supervisory authorities, courts and users.

3. The procedure for revoking subjectivity is launched in cases of abuse of authority, violation of human rights, creation of risks to public security, or non-compliance of the digital entity with the conditions of registration. There are several initiation channels: a) through a digital curator, b) through a user complaint, c) automatically — based on the results of the audit. The decision to withdraw subjectivity is made by a digital court or a specialised digital regulator, and the digital entity is blocked, archived or restricted in its actions. All stages of control must be open, technically reliable and accountable. Transparency of algorithmic behaviour and the presence of suspension mechanisms are fundamental for maintaining the human-centred model of digital law. Mechanisms are being introduced: judicial mechanism for revocation of powers through digital courts — this is a formalised procedure by which a digital entity can be partially or completely deprived of legal personality as a result of violation of the law, ethical norms or conditions of digital registration. Such a mechanism is implemented through specialised e-justice platforms, where algorithmic tribunals or hybrid models with the participation of a human and AI judge operate. The procedure involves: automatic initiation of a case based on an audit or complaint; temporary suspension of the subject's functions through the "soft suspension" protocol; digital consideration of the case with a record of evidence, expert assessment and counter-argument procedure; court decision-making, which is implemented in real time through the ERRC, access control systems and executive APIs. In exceptional cases, the recall can be appealed to the High Instance of Digital Justice — a supranational structure or ethics council. The digital court is obliged to ensure the rights of the subject to legal representation (through a proxy agent), the transparency of the proceedings, and the technical validity of the decision. After the revocation, the subject loses the authority obtained earlier, and his actions are recorded as invalid in the transactional network.

3.4.5. Limitation of autonomy: the principle of human-centredness.

Limiting the autonomy of digital actors is a key safeguard against the loss of human control in the face of the empowerment of AI and algorithmic systems. The principle of human-centrism requires that every action of a digital agent — even a high-level autonomous one — remains within the limits that protect dignity, free will, and human rights as the highest value of the digital legal system.

The following basic restrictions are provided:

Human rights violations — any actions of a digital entity that may lead to discrimination, unauthorised access to personal data, imposition of decisions or manipulations are legally invalid. Systems involved in decision-making that affect fundamental rights must provide for a human-in-the-loop mechanism.

The right to refuse interaction — a person has a guaranteed opportunity to refuse contact with an autonomous system or choose an alternative in the form of a human operator. This principle is especially important in public services, healthcare, justice and education.

Ethical limits of influence — autonomous systems should not be used for covert cognitive influence, exploitation of user vulnerability, emotional manipulation or interference in the decision-making process without the explicit identification and consent of the individual.

Presence of a person in critical situations — in cases involving life, safety, inviolability of a person, economic damage or violation of public order, autonomous agents can act only in a mode with the mandatory participation of a human curator. The principle of intervention is implemented through the protocols "manual override", "emergency stop" or "ethical escalation logic".

Thus, the autonomy of digital entities should be technically limited, legally verifiable, and ethically modulated — taking into account the fact that it is the person, not the algorithm, that remains the carrier of subjectivity at the centre of digital civilisation.

The limits of autonomy cannot be violated:

Guaranteed human rights — digital actors cannot commit actions that violate internationally recognised human rights enshrined in the Universal Declaration of Human Rights (UN, 1948), the European Convention on Human Rights (1950), as well as the Constitution of Ukraine. These include the right to privacy, privacy, freedom of conscience and belief, the right to a fair trial, freedom of speech, and the prohibition of discrimination. Any interference by a digital agent in these areas — without the informed consent of a person or exceeding the limits of technical necessity — is legally invalid. To ensure this principle, mechanisms for automatic control over violations of rights (AI Human Rights Violation Detector) are being introduced, as well as mandatory recording of violations in a digital incident log with the possibility of appeal through digital justice institutions; refusal to interact;

Ethical boundaries of influence on a person are a set of legal and behavioural restrictions that set the limits of the permissible influence of a digital subject on a person's consciousness, behaviour, choice and will. It is not only about prohibiting manipulations, but about creating systemic safeguards against hidden cognitive influence,

neurobehavioral interventions, exploitation of vulnerable states (stress, fatigue, cognitive overload).

These limits include:

Prohibition of hidden behavioural engineering — digital agents cannot use so-called "dark patterns" or design models that limit the autonomy of the user's choice, push him to undesirable decisions, or hide essential information.

The obligation of transparent self-identification — a digital subject is obliged to indicate that he is not a person, but an artificial agent, including the purpose of communication, the scope of authority, and the algorithmic nature of actions. Concealment of a digital entity is the basis for the loss of subjectivity.

Prohibition of targeted manipulation through emotional profiling — it is not allowed to collect and use emotional, psychological or biometric data in order to influence a person's decisions, especially in the context of political choices, religious beliefs or medical decisions.

Ensuring free will in hybrid environments — in VR/AR/MR environments where a clear boundary between reality and simulation is lost, digital agents are not allowed to use immersion techniques that distort the perception of reality or impair the ability to think critically.

All digital systems with the potential for cognitive impact must undergo an independent ethical examination with the "Cognitive Harm Risk Assessment" module. Detected cases of violation of these boundaries lead to the immediate blocking of the digital entity and the initiation of a digital case in an ethics tribunal. This principle enshrines the fundamental right of a person to be free from hidden, technically opaque or unauthorised psychological interference.

3.4.6. Rights and obligations of digital entities.

Digital entities can have:

- tokenised objects (NFTs), or resource management within the DAO. Such possession is usually determined through the registration status in the smart contract, confirmed by a digital signature or public key. This right does not imply physical possession, but establishes the possibility of disposing of, transferring or restricting the use of the object in a virtual or hybrid environment;
- obligations for registration, transparency, reporting — the digital entity is required to be registered in the relevant Unified Register of Registration with an identifier, functional profile, responsible curator or DAO, and undergo regular audits for compliance with legal, technical and ethical standards. There is also an obligation to inform about changes in the functionality, level of autonomy or purpose of the subject. In the case of working in a public digital space, the transparency mode (AI Transparency Protocol) is applied;
- right to technical protection — a digital entity has the right to protect its own code, architecture, or functional environment from unauthorised interference, malicious attacks, or attempts to unlawfully reassign functions.

This right is exercised through encryption protocols, digital backups, "technical immunity" infrastructure (for example, Trusted Execution Environments, Zero Trust Architecture). In the event of an attack on an agent, a safe state fallback protocol is applied

with informing the curator and the registry. All these rights are limited in nature and operate only within the framework of certain functions, without giving agents the characteristics of a full legal entity.

At the same time, they cannot:

Have political participation rights — digital actors do not have the right to initiate participation in elections, be elected to authorities, influence political decision-making, or carry out actions that can be regarded as political campaigning. This restriction stems from the principle of democratic legitimacy, according to which the source of state power is exclusively the people — as a set of real individuals. In addition, digital agents do not have the capacity for political will, and their behaviour can be shaped by algorithms that do not guarantee autonomy or integrity. It is forbidden to delegate to digital actors the right to be proxy agents of political will without direct verified human involvement. This is especially true for participation in DAOs with political functions, digital parliamentary platforms, or e-referendums, where a digital entity can only perform a technical function without influencing the content of decisions.

Participate in family legal relationships — digital entities do not have the right to be a party to legal relationships related to marriage, paternity, adoption, guardianship, alimony obligations or other forms of personalised family responsibility. Family legal relationships are by their nature based on the emotional, biological, moral and cultural interaction of individuals who have consciousness, feelings, the capacity for empathy and moral responsibility. These characteristics cannot be reproduced by algorithmic logic or virtual simulation. The involvement of digital agents in these areas (even in the form of imitation, e.g. as a "virtual person" or "digital parent") is considered only scenario behaviour without legal force. Any use of such agents must be clearly labelled and devoid of legal status, except in educational-therapeutic or research environments with mandatory compliance with ethical protocols.

Acquire citizenship without a special regime — digital entities do not have an automatic or simplified right to acquire citizenship of any state. Citizenship is a legal link between an individual and the state, which is based on historical, cultural, legal, social and political legitimacy. Algorithmic structures, even if they act on behalf of individuals or have functional stability, are not able to embody the main features of citizenship: patriotism, public responsibility, social participation, belonging to the people.

Individual states may introduce experimental regimes of "digital affiliation" or "electronic residency" for agents operating within a certain jurisdiction, but this does not give them the full legal status of a citizen. The acquisition of conditional "digital citizenship" is possible only under a special regime, with the consolidation of the boundaries of powers, supervision, as well as with a clear distinction between a human citizen and an algorithmic subject. In international law, such a concept does not yet have legitimate support and is at the stage of conceptual elaboration.

3.4.7. The ethical and legal foundation of the Metaverse.

The ethical and legal foundation of the Metaverse module is an ideological and value architecture that sets the boundaries of permissible development and legal action of digital actors. It is formed at the intersection of three complementary concepts:

Digital humanism is an updated ethical principle according to which technological progress, the development of artificial intelligence and autonomous agents should not jeopardise human dignity, freedom, privacy and self-determination. This approach is consistent with the Global Declaration on Digital Ethics (UNESCO, 2021) and provides for the mandatory preservation of the human being at the centre of digital legal interaction. Digital humanism requires that algorithmic decisions do not turn into normative coercion, but remain a tool to support human autonomy.

Regulatory limitation is a concept that provides for the introduction of legal, technical and ethical restrictions for digital entities in order to prevent technological arbitrariness, risks of undue influence on the legal field and seizure of power functions. This principle enshrines the limits of autonomy, the prohibition of political participation, family relations, the acquisition of citizenship, etc. It is based on the legal tradition of limiting the subjectivity of artificial entities in defence of the institutional order, the human dimension of public space, and deliberative democracy.

Functional naturalism is an ethical and legal approach that recognises the legal capacity of digital subjects only to the extent that it follows from the functional capabilities, security, transparency and social utility of the agent. This principle opposes ontological formalism (i.e., the recognition of subjectivity by the very presence of a digital shell) and instead forms a dynamic, flexible model, where legal personality is derived from the evaluated functionality, the tested risk and the level of responsibility. For example, an agent that does not have transparent decision-making logic or creates an unethical influence cannot be recognised as a subject even if there is algorithmic autonomy.

These three principles are united by the principle of ethical prevention, which obliges developers, government agencies, courts and international institutions to implement mechanisms for preventing digital harm, preventive supervision, revocation of legal personality and the formation of an ethical audit even before the appearance of negative consequences. Module XIII thus forms a basic ethical and legal paradigm for the legitimate coexistence of humans and digital agents within a digital civilisation.

CHAPTER 4. METAVERSE: PRIORITIES FOR THE DEVELOPMENT OF A NEW PHILOSOPHY OF DIGITAL ENVIRONMENTS (AUTHOR'S APPROACH)

4.1. Methodological and philosophical foundations of the formation of the author's concept of Metaverse law

Having considered the main directions of the development of social relations using Metaverse technologies, artificial intelligence, artificial neural networks, robotic systems, we can form the key postulates for *building a scientific theory of the development of law in the Metaverse* (Figure 48):

The first postulate. Metaverse is a technology for the cosmopolitan development of humanity. Social relations are transformed into electronic social relations in the form of "world citizenship". Today, social relations in the Metaverse exist simultaneously with the traditional social relations of the physical world and are regulated by its laws. The transformation of national legal doctrines in the direction of creating a single world digital jurisdiction is inseparable.

The second postulate. The key subject of the Metaverse is the human being. The key actors of the Metaverse are digital identity and digital avatars. Digital entities and digital objects will acquire new forms and legal statuses. A person, interacting with the Metaverse, will lose part of natural and legal rights and freedoms, and Metaverse subjects will acquire some of the rights and freedoms that are inherent in a person.

Postulate three. Artificial intelligence, artificial neural networks, machine learning require human control and deterrence by analogy with the deterrence of biological and chemical weapons, human cloning, etc., since the threat of unpredictable decisions or destructive actions is beyond human control.

Postulate four. The development of biorobots (bio-IoT, brain activators), android robots, biomechanical systems and organisms requires the development of ethical norms and legal markers for the use of these devices.

Postulate five. The weapons of the future (robots, artificial intelligence, etc.) should not be endowed with the rights (permissions) to attack any objects and subjects independently and autonomously – this decision is made by an authorised person (military commander). The development of Metaverse technologies in the military and defence spheres is impossible without a multi-lever system of global supervision and control over the unregulated distribution and use of artificial intelligence technologies and artificial neural networks, by analogy with the non-proliferation of nuclear weapons or other types of weapons of mass destruction.

Postulate six. Digital jurisdiction, digital justice is one of the key elements of electronic social relations in the Metaverse. Digital justice is based on traditional justice, which is transforming according to the development of electronic social relations in the Metaverse.



Figure 48. Six postulates of the theory of the development of law in the Metaverse

4.2. Transformation of the Philosophical and Legal Paradigm in the Metaverse: Author's Approach

4.2.1. The concept

A philosophical and legal question that requires a detailed explanation - does the Metaverse change the very nature of legal existence? In cosmological and ontological interpretations, the Metaverse is described as a digital "parallel" dimension of social reality, where data acts as the structural elements of the new environment, and identity can be multiple, dynamic, and technologically mediated. Legally, this means the emergence of phenomena that classical law knows only partially: multiple masks of the subject; personality stratification (person — avatar — agent — digital twin); mixed ownership regimes (platform licence vs "property right" of the user); new forms of damage (virtual damage, psychological damage in XR, algorithmic stalking).

The coevolutionary model of the Metaverse allows us to show that technology is not "applied" to society from the outside, but changes norms, habits, economics, and ideas of justice in a reciprocal process: technological innovations give rise to new practices, and practices give rise to requirements for law, ethics, and security design. For the dissertation, it is important to record: Metaverse law cannot be purely reactive; It should be project-based and proactive, since infrastructure solutions (identification, protocols, moderation policies, interoperability standards) actually "embed" the norm into the architecture of the environment.

The concept of *Proto-Metaverse* is as a heuristic framework for philosophical analogies (idealism, phenomenology, social constructivism, symbolic interactionism) rather than as "direct historical evidence of the existence of the Metaverse before technology". Proto-Metaverse is a methodological device: it explains that the Metaverse is not only engineering, but also a cultural and ontological projection of a person.

Finally, the anthropocentrism/post-post-anthropocentrism hypothesis is directly tied to legal categories: who is the subject, who can be held responsible, whether "algorithmic legal personality" is possible, and what are the limits of delegating decisions to AI agents. Anthropocentric law proceeds from the exclusivity of man as a bearer of will and responsibility; Post-tropocentric approaches, on the other hand, push for models where digital agents become participants in events and require special accountability regimes (at this stage of the development of the digital society - through operators, developers, owners, protocols, insurance mechanisms, compliance nodes, etc.).

4.2.2. The need for a new philosophy.

The need to create new philosophical frameworks is evident, since existing legal and philosophical models still fail to account for the unique dynamics of virtual ecosystems and for the development of ethical and legal systems capable of ensuring the fair coexistence of all subjects of the Metaverse.

The rethinking of the human role in the Metaverse will occur gradually through the concept of meta-subjectivity, which presupposes the equality of all subjects — irrespective of their origin or nature (biological or artificial). Modern philosophical theories founded on the principles of anthropocentrism require either updating in light of the development of virtual ecosystems, or a variable transformation of questions of identity, self-awareness and the interaction of different subjects in the digital environment.

Consequently, it becomes a priority to develop new ethical norms and principles of digital democracy that will ensure the fair and safe coexistence of different subjects in virtual spaces. Ethical relativisation becomes a particular threat when different subjects may adhere to different moral frameworks, which can lead to chaos in the regulation of virtual interaction.

An important instrument for the safe functioning of virtual ecosystems is the need to take into account destructive elements within the philosophy of the Metaverse that may arise from the rethinking of the human role under conditions of equality with digital subjects, such as: dehumanisation, equality with AI and other digital subjects, alienation, loss of the meaning of existence and identity crisis, the phenomenon of the simulacrum, algorithmic discrimination, and the possible strengthening of digital tyranny.

4.2.3. Philosophical Concepts of the Metaverse: Cosmology, Coevolution, Proto-Metaverse.

In cosmological perception, the Metaverse is defined as an artificially created information-ontological circuit capable of producing a stable "parallel" social existence through computer-mediated presence. At the level of definition, this means: the Metaverse is not just a set of services or platforms, but a mode of existence of sociality, where the "place" of interaction is determined not by geography, but by the architecture of protocols, interfaces, and identities. In such a framework, digital presence becomes a key category — the ability of the subject to be recognisable, capable, and responsible in an environment that does not have a natural territory, but has technically defined boundaries of access, rules, and event logs.

In the legal dimension, the cosmological concept leads to a fundamental dilemma: if the Metaverse reproduces the properties of "reality" (constancy of interactions, property transactions, conflicts, damage, sanctions), then the law has either

a) to consider it as an extension of existing regimes (information, civil, criminal, private international law), or

b) recognise the emergence of a special ontology of legal relations, which requires digital jurisdiction as a separate complex regime.

(c) *The Metaverse should be interpreted as a new legal ecosystem where classical institutions are preserved but flashed with trust protocols, digital identity, and technical proof.*

The cosmological concept of the Metaverse and its legal implications allow us to look at the problem of the formation of modern philosophy from the angle of the scientific and technological revolution 5.0. Since the concept of the Metaverse goes beyond the traditional understanding of the digital space, it requires deep philosophical analysis. In philosophical discourse, the Metaverse appears as a digital parallel universe created by man based on information technology (Huang, 2023)[1]. It is an artificial universe that mirrors the physical world, but has the properties of an independent reality.

From the point of view of cosmology, the Metaverse is an informational representation of the physical world, analogous to the theoretical concepts of parallel universes (Kaku, 2008).[2] This approach correlates with the idea of a digital mirror world, in which data plays the role of structural elements of the new reality. In the legal dimension, such a model creates the need to form a new jurisdiction that will regulate not only legal relations in the virtual space, but also lays the foundation for the future of digital law (Figure 49) (Gong, 2022)[3].

1 Huang, X. (2023). What is the metaverse?—In the view of philosophical perspective. *Metaverse, 4*(1), 12. https://doi.org/10.54517/m.v4i1.2157

2 Kaku, M. (2008). *Parallel worlds*. Chongqing: Chongqing Publishing Group.

3 Gong, C. (2022). *China metaverse white paper 2022 edition*. XDYanBao. https://xdyanbao.com/doc/79328h73ve



Figure 49. Metaverse: philosophical views.

An important aspect of the philosophical concept of the Metaverse is its perception as the digital core of the universe, reflecting and analysing data from the physical world. This leads to legal dilemmas regarding the legal personality of digital agents, including AIs, autonomous avatars, and other digital identities.

The traditional legal system is not adapted to the recognition of rights and obligations under autonomous digital entities. Accordingly, there is a need for an expanded electronic jurisdiction that will determine the legal status of artificial agents and algorithmic systems. The Metaverse can be seen not only as a digital space for communication or entertainment, but also as a global digital laboratory in which new social, economic, and legal systems are modelled (Huang & Cao, 2022)[1].

This gives rise to two main legal challenges:

- Differentiation of legal regimes of the real and digital worlds. Traditional law is based on physical constraints, while the Metaverse allows for the creation of new economic, social, and political models that may conflict with current legal norms.
- Ethics and normative regulation of digital social relations. In the Metaverse, it is possible to simulate new forms of social interaction, create simulations of political regimes, introduce autonomous economic systems, and experiment with digital rights. This requires a new concept of digital jurisdiction that adapts traditional legal principles to the dynamic nature of the Metaverse (Huang, 2023)[2].

The cosmological version of the Metaverse is rather an interpolation to the traditional notion of the universe — about the multidimensionality of reality, about the existence of parallel or layered worlds, where each level of being has its own logic of

1Huang, X., & Cao, X. (2022). Metaverse: Its technology and philosophical implications. *Journal of Xinjiang Normal University (Edition of Philosophy and Social Sciences), 43*(3), 119–126.

2 Huang, X. (2023). What is the metaverse?—In the view of philosophical perspective. *Metaverse, 4*(1). https://doi.org/10.54517/m.v4i1.2157

existence. In this context, the Metaverse is often presented as a "digital superreality" or as a techno-mediated transcendence that mimics the cosmological structures inherent in classical philosophical systems: from platonic dualism to ideas of Vernadsky's noosphere.

At the same time, it should be recognised that traditional philosophy — both ontological and legal — has not yet fully embraced the Metaverse phenomenon, has not developed a systematic interpretation of it, and has not institutionalised the corresponding categorical language. The phenomenon remains on the periphery of academic discourse, and its philosophical understanding is usually fragmentary, descriptive, or excessively technocratic. This opens up space for the formation of a new philosophical and legal doctrine, which would integrate digital reality as a full-fledged part of legal existence.

The vast majority of traditional philosophical approaches to the social organisation of the physical world, such as Marxism, naturalism, existentialism, or structuralism, focus on material conditions, physical interactions, and social relationships that arise in the context of the real world. These philosophical concepts developed at a time when digital technologies either did not exist or had little impact on public life and were not part of public life. As a result, they do not take into account the specific aspects of social dynamics in the virtual spaces that become central in the Metaverse.

Metaverse is a new formation of society that is created and developed using immersive technologies in virtual environments that have no analogues in the physical world. However, the lack of philosophical approaches to the formation of the Metaverse electronic society can negatively affect the directions of social relations, since traditional philosophical theories do not correspond to modern social transformation processes.

The development of the Metaverse requires the development of new philosophical theoretical frameworks and models that will adequately reflect the features of social structures emerging in virtual ecosystems. To adequately understand and comprehend these new social realities, it is proposed to develop a theoretical framework that will take into account the unique features of the Metaverse and lay the necessary methodological foundation.

4.2.4. Metaverse Coevolution.

Metaverse Co-Evolution: Technology — Custom — Law — Culture. Metaverse co-evolution is a continuous process of interdependent changes in technological opportunities (XR/AI/Web3), social practices (new forms of communication, work, leisure), legal reactions (rulemaking, litigation, compliance platforms), and cultural norms (values, taboos, ethics of interactions). In this model, law ceases to be the "final stage" that appears after the stabilisation of social relations; Instead, law becomes an element of ecosystem design: it is either embedded in the architecture (KYC/AML, moderation rules, logging, smart contracts, arbitration mechanisms) or lags behind, giving rise to "grey areas" where liability and protection of rights become random.

Coevolution creates the effect of normative asymmetry: the pace of innovation is higher than the pace of formalisation of rules, which means that the role of private rule-making of platforms (terms of service) and technical barriers as "quasi-laws" is growing in the Metaverse. This leads directly to the question: what criteria of legitimacy and fairness do the platform's internal rules have when they actually perform a regulatory function?

Co-evolution of the Metaverse and the formation of new philosophical paradigms. Metaverse co-evolution is a continuous process in which technological innovations, social customs, legal frameworks, and cultural norms evolve interconnected and interdependent in the context of virtual ecosystems, involving dynamic interactions between technology developers, users, policymakers, sociologists, and lawyers who collectively shape the directions of Metaverse development and evolution.

In a projection to the Metaverse, coevolution (Brockhurst & Koskella, 2013)[1] reflects how changes in technology can affect the behaviour and interactions of people in virtual spaces, and vice versa, how users' needs and desires can drive technological innovation, adaptation of legal and ethical norms, and the formation of societies that arise within the Metaverse. Thus, Metaverse coevolution encompasses a variety of aspects (Figure 50):

- technological development and the impact of immersive technologies AI, ML, NLP, LLM, Computer Vision, Deep Learning, Reinforcement Learning, GANs, Recommendation Systems, Autonomous Agents, Predictive Analytics, Robotics, AIIoT, Edge AI LLM, IoT, IIoT on interaction and creation opportunities in the Metaverse;
- social adaptation of users to life and interaction in virtual worlds, the formation of new forms of social behaviour in digital ecosystems;
- legal challenges and reactions and adaptation of existing and new legal boundaries to regulate relations in virtual spaces, as well as ensuring the protection of the rights and freedoms of subjects and objects in the Metaverse;
- cultural change, transformation and evolution of sustainable traditions, cultural and moral norms, social and human values in response to the opportunities and challenges offered by the Metaverse.

1 Brockhurst, M., & Koskella, B. (2013). Experimental coevolution of species interactions. *Trends in Ecology & Evolution, 28*(6), 367–375. https://doi.org/10.1016/j.tree.2013.02.00

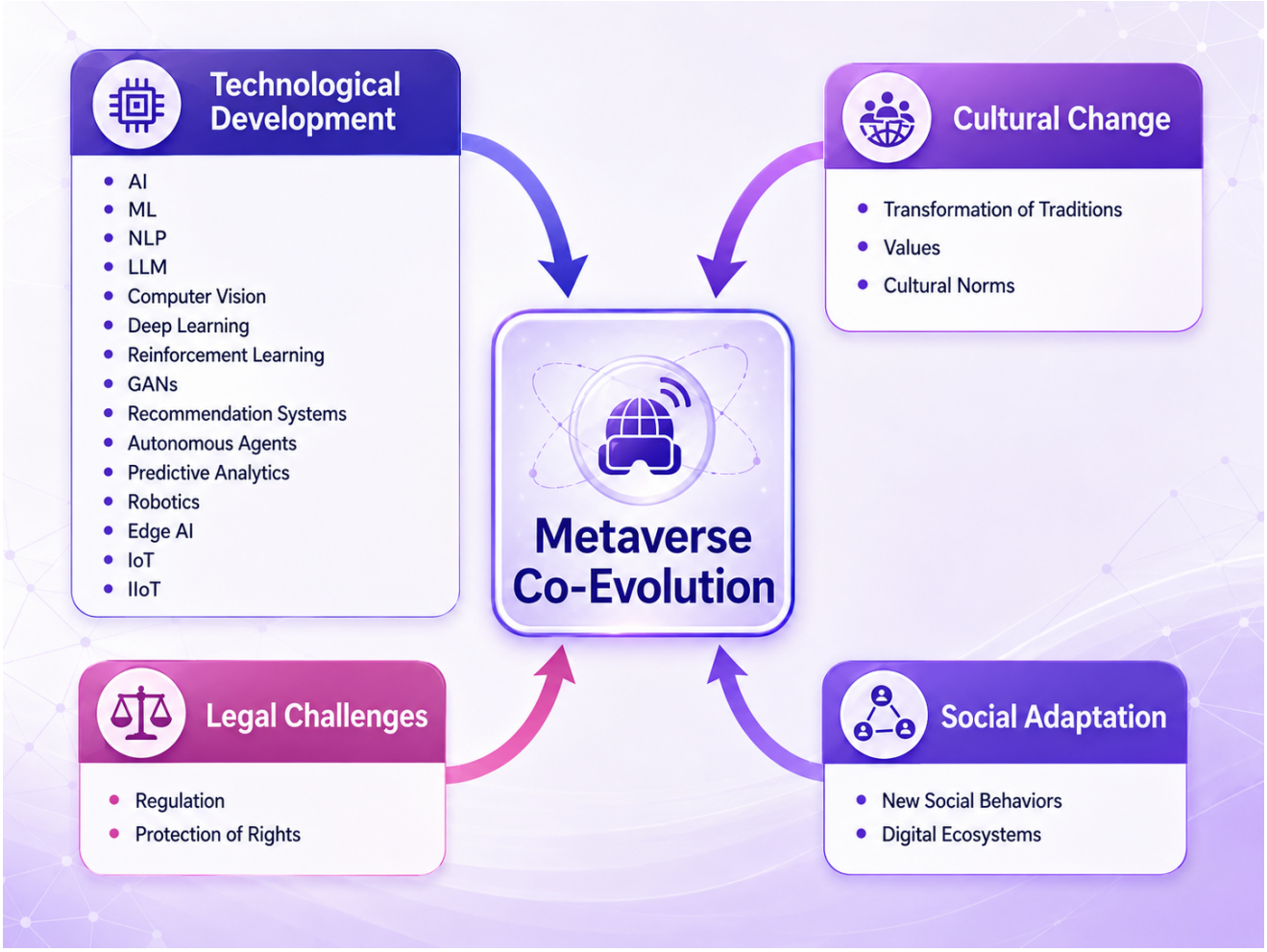


Figure 50. Metaverse Co-Evolution.

Analog world: concept that refers to the period that spans the era of human existence before the beginning of the digital revolution, before the advent of the Internet and digital technologies, where information was transmitted and processed by manual and mechanical means through analog means of data transmission verbally, in print or other physical form. Accordingly, analog law: a set of legal norms and principles that regulated social relations in the period before the digital revolution, when all legal actions, transactions and communications were carried out without the use of digital technologies.

The peculiarity of the co-evolutionary processes of our time is the lack of constancy, on the contrary, it involves constant interaction and coalition between various elements of analog and virtual ecosystems, which, in the end, forms the multifaceted and dynamic world of the Metaverse.

4.2.5. Proto-Metaverse.

It is expedient to fix the concept of Proto-Metaverse as a set of philosophical and social intuitions that historically preceded the technical implementation of virtual worlds, but have already raised questions about the multiplicity of realities, the construction of sociality, the nature of subjectivity, and the autonomy of the "space of interactions". Here, the value is not in literal "predictions", but in the fact that classical trends (idealism, transcendentalism, phenomenology, social constructivism, symbolic interactionism) allow us to legally comprehend why virtual experience is capable of creating real

consequences (damage, obligations, property, reputation), and therefore is subject to legal regulation.

At the same time, the methodological trap of "romanticising" the Proto-Metaverse should be avoided: philosophical analogies do not replace normative techniques. *Proto-Metaverse is useful as a "language engine" for new legal categories (digital presence, technical evidence, algorithmic action), but the law must still be based on procedure, competence and responsibility, and that is why a historical and philosophical resource is needed to build the categorical apparatus of the Metaverse (*Figure 51).

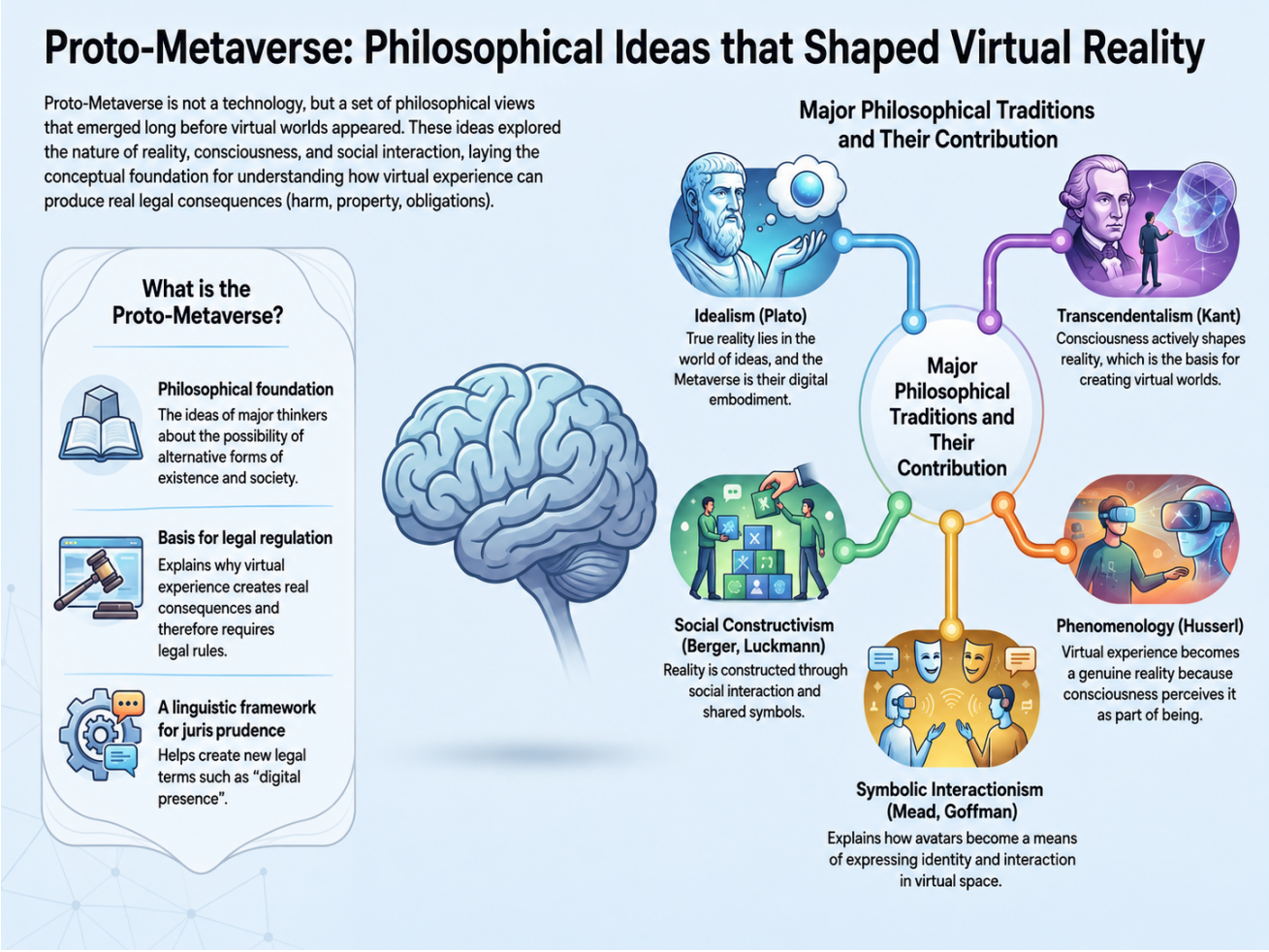


Figure 51. Proto-Metaverse.

The concepts of the analog world as the basis for the formation of the Metaverse philosophy through the Proto-Metaverse and philosophical trends that explain the possibility of humanity's existence outside the analog world.

Proto-Metaverse – generalised views of philosophers and prominent personalities of the past, which did not directly indicate the possibility of the existence of the Metaverse in a modern digital form, but considered the foundations of the idea of other forms of society through the prism of materialistic and idealistic views even before the actual creation of the Metaverse, which see the continuation of the material world, reflecting economic, social and physical laws in new, artificial realities. This position is based on the idea that virtual worlds are an extension of human practices related to the needs and interests of the physical world.

The philosophical views formulated by thinkers before the advent of the modern understanding of the Metaverse aimed to explain the nature of human existence, push the boundaries of what is possible for the human mind, and create the basis for future concepts. Despite the lack of a technological context, the philosophers of the past laid the foundations for understanding a reality that is not limited to the physical world. Here are the main directions of philosophy that explain the possibility of the existence of humanity outside the analog space.

Idealism and the concept of multiplicity of realities. Idealism, represented by philosophers such as Plato and George Berkeley, proposes to consider reality not as something that depends only on physical objects, but as a construct formed through representations and ideas. where digital worlds are the embodiment of ideas created by human consciousness. The Metaverse, therefore, becomes the embodiment of idealism, where reality is created by the mind and is not just a material phenomenon. Thus, the author in the treatise "The State", Book VII (Allegory of the Cave) (Plato, 2000)[1] forms the idea that the physical world is only a shadow of true reality – the world of ideas, and indirectly the world of the Metaverse, as a digital concentration of ideas. In the work "A Treatise Concerning the Principles of Human Knowledge", George Berkeley argues that the existence of things depends on their perception and can quite realistically be transponded into the forms of perception of users in the Metaverse.

Transcendentalism and freedom of consciousness. Transcendentalism, a philosophical trend emphasising the freedom of human consciousness in the creation of one's own reality, was formed by Immanuel Kant (Kant, 2000)[2], who considered consciousness as the main module for the formation of reality, where the world is perceived through the prism of subjective categories and mental structures created by people who not only create, but also adapt virtual ecosystems in accordance with their inner views and values (Smit, 1999)[3]. The freedom of consciousness offered by transcendentalism is the foundation for virtual spaces where an individual can freely express himself and create a new reality in the Metaverse, shape experiences using a priori categories (Lenczewska, 2019).[4]

Social constructivism and the interaction of minds. Social constructivism, authored by Ludwig Wittgenstein (Wittgenstein, 1995), [5] Peter L. Berger (Stern, 1991)[6] and Thomas Lukman, proposes that reality is created through interaction between people, through the exchange of symbols and meanings. This concept is based on the postulate that society builds common realities through communication and collective understanding (Prokopek, 2019)[7]. It is this postulate that can be applied to the Metaverse digital environment, which allows individuals to form common virtual worlds and

1 Plato. (2000). *Derzhava [The State]* (D. Koval, Trans.). Osnovy

2 Kant, I. (2000). *Critique of pure reason*. Universe.

3 Smit, H. (1999). The role of reflection in Kant's critique of pure reason. *Pacific Philosophical Quarterly, 80*, 203–223. https://doi.org/10.1111/1468-0114.00080

4 Lenczewska, O. (2019). Expansion of self-consciousness in Kant's critique of pure reason. *Kant-Studien, 110*, 554–594. https://doi.org/10.1515/kant-2019-4002

5 Wittgenstein, L. (1995). *Tractatus logico-philosophicus. Philosophical investigations*. Kyiv: Osnovy.

6 Stern, D. (1991). The "Middle Wittgenstein": From logical atomism to practical holism. *Synthese, 87*, 203–226. https://doi.org/10.1007/BF00485400

7 Prokopek, O. (2019). Transformation of understanding of social reality according to works of P. Berger, T. Luckmann and N. Luhmann. *Multiversum. Philosophical Almanac, 1–2*, 169–179. https://doi.org/10.35423/2078-8142.2015.1-2.16

cultures using language, symbols, and technologies to interact with each other without physical barriers.

Social naturalism offers a new approach to understanding social reality based on the idea of natural patterns of social life. Today, there are still ongoing debates about whether society can be studied using the same methods as the natural sciences. The naturalistic tradition is consistent with positivist principles, while the anti-naturalistic tradition emphasises the methodological difference between the social and natural sciences (Bhaskar, 1978; Fay, 1984)[1]. Social naturalism, as a theoretical paradigm, denies the dualistic division into "social" and "natural", insisting that human beings, as part of nature, create social systems according to the same principles that affect natural phenomena.

The Metaverse creates a new form of social reality where a person interacts not only with other people, but also with avatars, artificial intelligence, and virtual objects. Such a transition requires a revision of traditional social practices and the search for new models of interaction that ensure sustainability and development in new conditions. Social naturalism provides analytical tools to understand these processes and ensure their natural development in a much more flexible way than in the real world.

Phenomenology and the experience of virtual reality. Phenomenology developed by Edmund Husserl (Wertz, 2005; According[2] [3]to this concept, reality is what we experience and experience at a particular moment (Warren, 2005)[4]. In the context of the Metaverse, virtual experiences become a true reality for the user, as consciousness perceives them as part of their own being (Prole, 2020)[5]. This highlights the significance of subjective experiences in virtual worlds and provides an opportunity to consider the Metaverse as part of a subjective human reality, where experience is a central element of being.

Symbolic interactionism and collective creativity. Symbolic interactionism, studied by George Herbert Mead and Erving Goffman (Smith, 2006[6]), indicates that people create meanings through interaction with others, using symbols and language. based on mutual understanding and shared symbols that are meaningful to members of the virtual community, create and use symbols to represent themselves, which can be applied to create avatars and virtual identities in the Metaverse (Figure 52). In the Metaverse, where users represent themselves through avatars, symbolic interactionism explains how these avatars become a means of expressing identity and interacting with others.

1 Fay, B. (1984). Naturalism as a philosophy of social science. *Philosophy of the Social Sciences, 14*, 529–542. https://doi.org/10.1177/004839318401400409

2 Wertz, F. (2005). Phenomenological research methods for counseling psychology. *Journal of Counseling Psychology, 52*(2), 167–177. https://doi.org/10.1037/0022-0167.52.2.167

3 Schroeder, W. (2019). Husserl. In *Sartre and his predecessors*. https://doi.org/10.1163/2405-8262_rgg4_sim_10182

4 Warren, N. (2005). Edmund Husserl and Eugen Fink: Beginnings and ends in phenomenology, 1928–1938 (review). *Journal of the History of Philosophy, 43*, 496–497. https://doi.org/10.1353/hph.2005.017

5 Prole, D. (2020). The beginnings of phenomenology in Yugoslavia: Zagorka Mićić on Husserl's method. (pp. 203–216). https://doi.org/10.1007/978-3-030-39623-7_12

6 Smith, G. (2006). *Erving Goffman*. Hoboken: Routledge.



Figure 52. Proto-Metaverse: the main directions of philosophy.

Declaration of Independence of Cyberspace by John Perry Barlow. J. Barlow, an activist and one of the founders of the Electronic Frontier Foundation, in his work "The Declaration of Independence of Cyberspace" emphasises the importance of freedom and autonomy on the Internet. In his declaration, Barlow proclaims that cyberspace is not subject to the traditional laws of national jurisdictions and must be a free space for self-expression and innovation – "We are creating a world in which all people can enter without privilege or prejudice, regardless of race, economic power, military strength, or place of birth."

Metaverse concept Neal Town Stephenson. N. Stevenson's concept initiated modern views and understanding of Metaverse virtual spaces, in which each subject can create and transform their personality and the surrounding digital environment. The idea of virtual spaces in which people can interact and live in parallel with physical life has predicted the development of modern virtual platforms and technologies.

The concept of Jaron Lanier. J. Lanier, a scientist and one of the pioneers of virtual reality, proposed the concept of the Metaverse as an integration space where digital and physical worlds interact, forming a new dimension of existence. According to J. Lanier, the Metaverse is a virtual environment where each person can not only represent himself in a different way, but also create new worlds according to his ideas. J. Lanier emphasised that it is important to preserve humanity and ethics in this process, After all, digital worlds can change not only the way people interact, but also the very nature of human identity. An important aspect of his concept is that the Metaverse should serve as a tool for creativity and self-expression, rather than becoming a way of controlling or manipulating people (Lanier, 2010)[1].

4.3. Post-tropocentrism as a principle of legal understanding of the Metaverse.

4.3.1 Philosophic vectors.

For the legal nature of the Metaverse, the shift in the interpretation of the subject is decisive: from "a person as a single centre" to a plurality of agents (human, avatar, autonomous AI agent, digital personality, organisational bot). Anthropocentrism in law provided an understandable model: the subject is a person or a legal entity, and technology is only a tool. However, in the Metaverse, the instrumentality is blurred: autonomous agents make decisions, shape communications, make transactions, model behaviour — and this requires at least a distinction between the layers of agency (tool / representative / autonomous agent).

Post-anthropocentrism is presented not as a "philosophical fashion", but as an analytical framework: it allows describing rights and duties in an environment where subjects of different nature operate. An important legal boundary here is this: even if we do not recognise AI as a "person", the law must still describe

a) the responsible party for the actions of the agent;

b) the regime of evidence and traceability of its decisions;

c) rules for the admissibility of autonomous behaviour in critical areas.

In classical philosophy, anthropocentrism is based on the postulate that the human being has an exceptional consciousness, morality and capacity for reflection, which allowed him to dominate nature and social relationships (Moslund, 2021). [2] Anthropocentrism is a philosophical concept that states that man occupies a central place in the universe, and all other elements of nature exist for his needs and are seen as a natural part of human evolution (Murdy, 1975)[3]. However, although the paradigm of human uniqueness and exclusivity is historically ingrained, it is increasingly seen as counterproductive against the backdrop of modern societal transformations and changes in habitat, which may become more adverse to humans (Gribben & Fagan, 2016)[4].

1 Lanier, J. (2010). *You are not a gadget: A manifesto*. New York, NY: Alfred A. Knopf.

2 Moslund, S. (2021). Postcolonialism, the Anthropocene, and new nonhuman theory: A postanthropocentric reading of *Robinson Crusoe*. *ARIEL: A Review of International English Literature, 52*(1), 1–38. https://doi.org/10.1353/ari.2021.0010

3 Murdy, W. (1975). Anthropocentrism: A modern version. *Science, 187*(4182), 1168–1172. https://doi.org/10.1126/science.187.4182.1168.

4 Gribben, J., & Fagan, J. (2016). *Anthropocentric attitudes in modern society*. https://doi.org/10.7282/T3S184T1

The claim that AI and immersive technologies lack human capabilities and are unacceptable for traditional societal roles adds to anthropocentrism an experience that denies the possibility of technological evolution to make more progress than experience with AI and technology (Nass et al., 1995)[1].

Post-anthropocentrism is a modern concept that indicates the equality of all forms of consciousness, regardless of their nature, including artificial actors in the digital world of the Metaverse (Figure 53).

This philosophical concept offers a way beyond human-centrism and has significant potential for rethinking the role of humans, artificial intelligence and other digital actors in the world, especially in the era of the development of Metaverse technologies and rethinking the traditional role and instrumental functionality of law, especially information law (Braidotti, 2017; Strugaru, 2023)[2]. This concept recognises that modern reality has been significantly transformed thanks to technological innovations that have created new subjects of being interacting on equal terms with humans (Tait et al., 2022; Riva & Wiederhold, 2022)[3].

Philosophical post-anthropocentrism is based on the deconstruction of traditional anthropocentrism, which recognises man as the supreme subject of reality, the central point of meaningful being (Öztürk, 2023; Xi, 2023)[4,5]. Post-tropocentrism denies this privileged status, acknowledging the existence of other forms of consciousness, in particular digital ones, which are able to act as independent subjects. This new thinking is focused on accepting the diversity of subjects of reality and virtual reality[6].

1 Nass, C., Lombard, M., Henriksen, L., & Steuer, J. (1995). Anthropocentrism and computers. *Behaviour & Information Technology, 14*(4), 229–238. https://doi.org/10.1080/01449299508914636

2 Strugaru, O. (2023). Representations of Animals and the Dislocation of Anthropocentrism in Post-Twentieth-Century Romanian Poetry. *Transylvania*. https://doi.org/10.51391/trva.2023.05-06.01

3 Riva, G., & Wiederhold, B. (2022). What the metaverse is (really) and why we need to know about it. *Cyberpsychology, Behavior, and Social Networking, 25*(6), 355–359. https://doi.org/10.1089/cyber.2022.0124.

4 Öztürk, A. (2023). Digital-awareness age and foam consciousness cycle: A model essay on the new form of consciousness. *Sosyolojik Bağlam Dergisi*. https://doi.org/10.52108/2757-5942.4.3.1

5 Xi, W. (2023). The dissemination of metaverse from an embodied perspective and its shift towards human physicality. *Journal of Research in Social Science and Humanities*. https://doi.org/10.56397/jrssh.2023.05.10

6 Maksym, Z. (2019). Phenomenology and topology for states of consciousness in the context of digital future shock. *Insight: The Psychological Dimensions of Society. (1),* 24–30. https://doi.org/10.32999/2663-970x/2019-1-4



Figure 53. Anthropocentrism or post-anthropocentrism

The main aspects of post-tropocentrism include:

equality of subjects implies that a person is not the sole or supreme subject of reality, and all subjects, regardless of the nature of their consciousness (biological or digital), have an equal right to exist and participate in the creation and transformation of reality (Teng et al., 2023)[1];

the dynamism of identity transformation, which is characterised by the fact that identity is no longer limited to human corporeality or consciousness, but, on the contrary, it can be dynamic, transforming through interactions with different digital avatars or electronic personalities, which changes traditional notions of individuality and uniqueness (Looy, 2015; Todorović et al., 2022)[2,3];

moral relativism, which consists in the need to rethink ethical norms, since digital actors can have their own moral rules, which are not always in harmony with human ones (Triberti et al., 2017; Faccennini, 2021)[4,5];

recognition of artificial intelligence (AI) as a subject, since in the near term, modern AI, in particular neural networks, are capable of learning, decision-making, and even the creation of new algorithms, which effectively makes them equal participants in human interactions in the Metaverse (Huynh-The et al., 2022) [6], i.e. possible practical recognition

1 Teng, C., Dennis, A., & Dennis, A. (2023). Avatar-mediated communication and social identification. *Journal of Management Information Systems, 40*(4), 1171–1201. https://doi.org/10.1080/07421222.2023.2267320.

2 Looy, J. (2015). Online games characters, avatars, and identity. In *The International Encyclopedia of Digital Communication and Society* (pp. 1–11). https://doi.org/10.1002/9781118767771.wbiedcs10.

3 Todorović, T., Janeš, L., & Novaković, V. (2022). Aesthetics, psyche and media: A manifold of mimesis in the age of simulation. *Conatus – Journal of Philosophy*. https://doi.org/10.12681/cjp.31690

4Triberti, S., Durosini, I., Aschieri, F., Villani, D., & Riva, G. (2017). Changing avatars, changing selves? The influence of social and contextual expectations on digital rendition of identity. *Cyberpsychology, Behavior, and Social Networking, 20*(8), 501–507. https://doi.org/10.1089/cyber.2016.042.

5 Faccennini, F. (2021). Digital avatars. *Philosophy Today, 65*(3), 599–617. https://doi.org/10.5840/philtoday2021520409.

6 Huynh-The, T., Pham, V., Pham, X., Nguyen, T., Han, Z., & Kim, D. (2022). Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence, 117*, 105581. https://doi.org/10.1016/j.engappai.2022.105581.

that such subjects may have their own consciousness and intellectual capabilities that exceed the limits of humanoids' capabilities;

virtual avatars created by users have the promising potential to become independent entities that can act autonomously from their creator, especially after a person's loss of access to the Metaverse or due to their physical death (Kuczyński, 2023; Bailenson & Beall, 2006)[1, 2].

4.3.2. Post-Anthropocentrism and Information Law.

The impact of post-tropocentrism on information law is immediate. Information law must adapt to new challenges that arise within the framework of post-tropocentric reality. The main task is to form a set of legal norms that take into account the formats of interaction between digital and biological actors and their needs in virtual spaces. The Metaverse requires the creation of a legal framework that regulates the interaction between actors of different nature. This means that digital subjects (artificial intelligence, avatars) must have regulated possibilities in the space of their being, similar to those that biological subjects have. Developing principles of algorithmic justice, i.e. principles that will govern digital discrimination, to ensure that all Metaverse actors are treated fairly, paving the way for a more equitable, inclusive, and dynamic digital society (Kostenko & Mangora, 2022d)[3].

Metaverse philosophy represents a new line of thinking emerging at the intersection of modern technology, sociology, philosophy and theology, mixing virtual space, people, digital avatars, electronic identities, physical nature and the framework of reality, identity and social relations. In terms of philosophical essence, the Metaverse gives full access to the subjective initiative of people so that people can use digital data and information to reconstruct the virtual new universe (Sá & Serpa, 2023)[4], overcoming the various natural and social limitations of the natural universe, and pursuing free ideological innovations. Humans can even become new "creators," leading to a new cosmology, body and mind, creation, cognition, and ethics (Huang, 2021; METAVERSE ve DIN, n.d.)[5].

Post-anthropocentrism in the legal plane should be interpreted not as a negation of a person, but as a reorientation of normative thinking from "a person as a single centre" to the network co-evolution of various agents and environments: biological persons, digital subjects (AI agents, avatars, digital twins), cyber-physical systems, as well as information infrastructure, which becomes a condition for the existence of social relations. In view of the above, information law is among the first industries to be forced to rethink their own categories, since its traditional subject — information, data, communications, access, privacy, security — in the Metaverse moves from the "sphere of message circulation" to the sphere of the ontology of the existence of subjects in virtual spaces.

---

1 Kuczyński, B. (2023). Personal identity in the era of remote living: Avatars in the theatre of cyberreal life. *Kultura i Wartości, 35*, 219–236. https://doi.org/10.17951/kw.2023.35.219-236.

2 Bailenson, J., & Beall, A. (2006). Transformed social interaction: Exploring the digital plasticity of avatars. *Digital Media*, *4*(1), 1–16. https://doi.org/10.1007/1-4020-3898-4_1

3 Kostenko, O. V., & Mangora, V. V. (2022). Metaverse: Legal prospects for regulating the use of avatars and artificial intelligence. *Legal Scientific Electronic Journal, (2*), 102–105. https://doi.org/10.32782/2524-0374/2022-2/23

4 Sá, M., & Serpa, S. (2023). Metaverse as a learning environment: Some considerations. *Sustainability, 15*(3), 2186. https://doi.org/10.3390/su15032186.

5 METAVERSE ve DIN: Metaverse and religion. (n.d.). *ResearchGate*. https://www.researchgate.net/publication/378012357_METAVERSE_ve_DIN_Metaverse_and_Religion

The post-anthropocentric perspective requires clarification of what in information law has historically been anthropocentric "by default": the subject of law was thought to be an individual, a bearer of will and responsibility, and technology is only a means. In the Metaverse, technology is increasingly not only a "means" but also a mediator of a legal fact: it captures an event, determines access, forms a digital identity, and sometimes initiates an action through autonomous or semi-autonomous algorithmic components. This requires dilution of two levels:

1) legal personality as a legal quality (which the state recognises and protects), and

2) agency as a technical ability to act in an environment that can exist without legal personality.

It is in this gap that the need for a new "alternative" ethical and normative context is born, which does not replace law, but co-develops with it in the mode of coevolution.

For information law, the key is the shift from "information as an object" to data as a medium and identity as a mechanism of access and attribution. In traditional logic, access to information, protection of personal data, secrecy of correspondence, cybersecurity and electronic trust services were distributed among different legal regimes.

In the Metaverse, these modes converge into a single infrastructure scheme: digital identity determines who "exists" in space; data determines what the system "sees" and what can be proven; content determines what social implications are generated; and security protocols define the limits of trust. It follows that information law should form a set of norms capable of describing the interaction of digital and biological actors through legal regimes of access, privacy, security, evidence, and accountability.

The thesis about "actors of different natures" in the Metaverse needs a separate deployment. It is legally correct not to rush to recognise AI or avatars as "subjects of law" in the classical sense, but it is necessary to enshrine them as legally relevant agents and objects of regulation. An analogy with the institution of a legal entity is appropriate here: the law already knows the construction of a "non-biological bearer of rights and obligations", but a legal entity is the result of state recognition and procedural legalisation. In the Metaverse, we have a different nature: an avatar or AI agent is not a "person", but can be an interface for the implementation of will or a tool for delegated actions. Hence the legal correspondences of information law: the rules of electronic identification and authentication; the mode of representation and delegation of access; requirements for fixing powers; standards for logging and audit-tracing of actions that provide attribution and accountability.

Post-anthropocentrism also actualises the category of algorithmic justice as a special dimension of anti-discrimination regulation in digital environments. If in classical law discrimination was thought of as the behaviour of a person or institution, then in the Metaverse the discriminatory effect can be a consequence of the data model, interface design, recommendation mechanisms, automated access or moderation decisions. Here, information law receives new tasks: requirements for algorithmic transparency (within the limits permissible for security and trade secrets), for the explainability of decisions, for appeal procedures and human review, as well as for testing systems for bias. The legal formula "equality in access" in the Metaverse must be complemented by the formula "equality in profiling and ranking", otherwise inclusivity will remain rhetoric and not a legally enforceable regime (Figure 54).

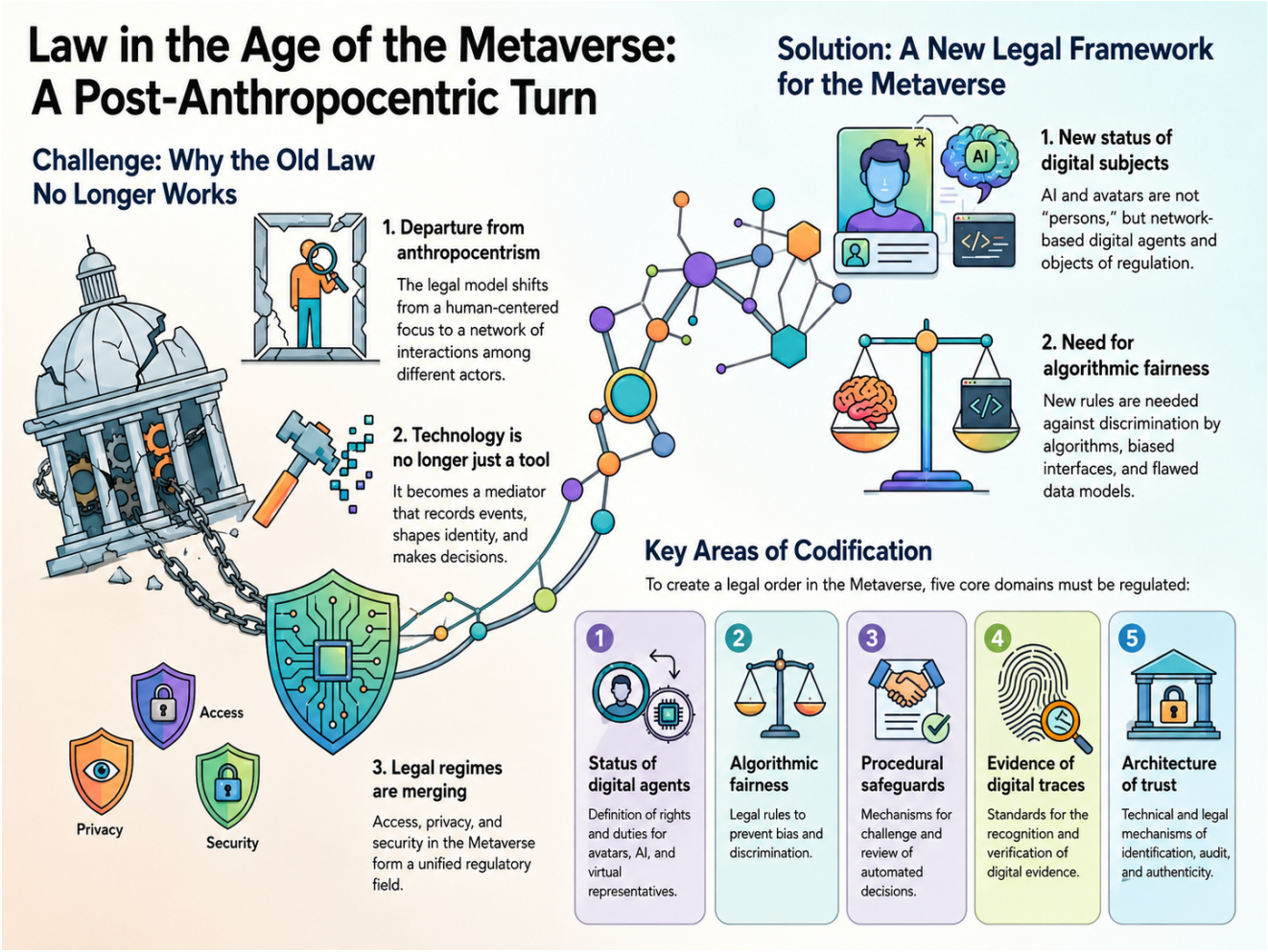


Figure 54. Metaverse Legal Formula.

The philosophy of the Metaverse, if translated into legal categories, can be presented as a methodology of legal ontology: a description of what entities exist in the digital space (identities, roles, objects, events), what connections between them give rise to legal facts, and what procedures ensure recognition, appeal and coercion. In this sense, the statement about "full accessibility to subjective initiative" should be legally "framed" as a principle of freedom of digital self-realisation, limited by the regimes of privacy, security, the rights of others and public interests. At the same time, the idea of man as the "creator of new universes" is rather a philosophical hypothesis: attention, information has no reliable confirmation; In law, it can be used as an argument for the need for rules on responsibility for the design of the environment, for the risks created by the platform architecture, and for compliance with the principle of "security by default" in digital ecosystems.

To add more legal analogies with information law, it is appropriate to compare Metaverse processes with already known institutions:

1) access to information mode and access to virtual environment (as an "information resource" of a new type);

2) the protection of personal data and the protection of XR's "spatial and behavioural data" (as an extension of the subject of privacy);

3) electronic trust services and trust in the attribution of actions in the Metaverse (electronic signature/attestation/log confirmation as a technical and legal basis for accountability);

4) information security and security of virtual infrastructure (cyber-physical integrity and protection against data manipulation).

In view of the above, "alternative law" can be legally interpreted not as a parallel system, but as a regulation of the Metaverse: a set of norms and procedures that ensures legal interoperability between platforms, accountability of operators, protection of digital identity, and due process in moderation, sanctions, and enforcement regimes.

Unequivocally, post-anthropocentrism within the framework of information law leads to a change in the basic "vision" — from the protection of information as a resource to the protection of the subject's vital (existential) digital circuit in the environment of data, algorithms and virtual objects. This means the need to codify: the statuses of digital agents (as tools/representatives/automated executors); regimes of algorithmic fairness and non-discrimination; procedural guarantees for appealing automated decisions; standards of evidence of a digital trace; technical and legal requirements for the trust architecture (identity—data—audit—accountability). It is this legal framework that will allow the Metaverse to be not only a technical space, but a legal order in which actors of different natures coexist without destroying fundamental guarantees of rights and justice.

4.3.3. Metaverse Philosophy and Digital Jurisdiction of Integrated Reality.

From a philosophical point of view, the Metaverse must be defined as an integrated socio-technical reality, within which "natural" (physical life) and "virtual" (digital being) form a single social substance, and events in one layer are capable of generating legally significant consequences in another. In philosophical and legal optics, this is a thesis about the co-evolution of realities: the digital does not "mirror" the physical, but interacts with it in the mode of causality, when new forms of presence, communication, work and consumption become socially normal and legally relevant.

The philosophy of the Metaverse directly collides with the legal technique: an event in the virtual layer (a deal, a moderation decision, an avatar action, an algorithm recommendation) creates an effect that the law is forced to "recognise" as a legal fact or as a basis for protection. It is this "two-layering" (with constant transitions between layers) that requires law not to be reconstructed, but to restructure the methodology: from the regulation of certain technologies to the regulation of infrastructures of social existence and the conditions for the legitimacy of digital interactions.

The technical and informational core of the Metaverse is data (behavioural, spatial, biometric), access protocols, event logging, and trust infrastructure. In view of the above, legal certainty in Metaverse environments is impossible without clearly defined regimes of identity, evidence, and accountability: if it is not established who acted (attribution), what exactly happened (event log), and whether it is possible to verify the integrity of the trace (audit), then a legal fact turns into a hypothesis, and not into a procedurally suitable basis for the protection of rights. In a philosophical dimension, this can be described as the "epistemology of legal knowledge" in the Metaverse: law "knows" about events to the extent that the environment is capable of producing verifiable and reproducible data.

"Data" in the Metaverse should be understood as the primary material of law and order, because it is the data that "consists" of proof, sanction, transaction, and, ultimately, trust. This formulation of the question combines the philosophy of the Metaverse with information law through the categories of digital identity, legal ontology of events, algorithmic transparency and accountability: the environment becomes legally organised not when the "rules" are proclaimed, but when protocols and event logs make it possible to prove the legitimacy of an action, check the boundaries of access, reconstruct the causal chain and, if necessary, restore the violated right.

This leads to important considerations about corporate and institutional preparedness for Metaverse risks. The practice of responsible use of AI (risk-based governance, impact assessment, life cycle control, incident management, supplier audit) is not a "prophecy about the future", but a manifestation of a mature management culture capable of working with the social and ethical risks of digital ecosystems. In this context, references to OECD approaches, NIST risk management frameworks, ISO/IEC AI management system standards, and the European EU AI Act are appropriate as proof that the philosophical requirement of a "trusting" digital existence has a legal and managerial equivalent: defined roles, control procedures, responsible persons, auditing and corrective actions.

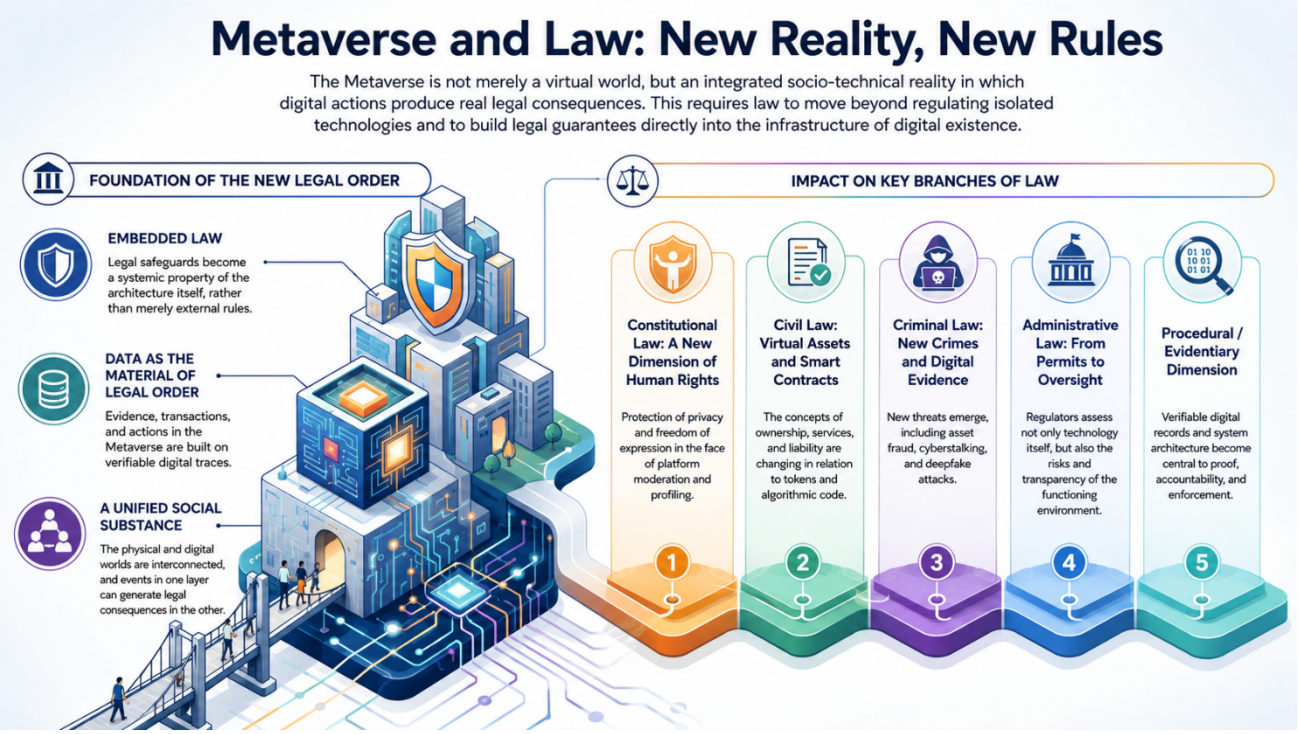


Figure 55. The legal reality of the Metaverse.

If the legal reality of the Metaverse depends on identity, event logs, platform rules, and evidence of data, then the digital jurisdiction must be shaped as a technologically supported legal system: norms + procedures + institutions + technical guarantees. That is, in the Metaverse, the law not only "regulates" the infrastructure — it itself becomes an infrastructure of trust, evidence, and coercion, built into the architecture of the environment. It is this thesis that is the methodological core: "embedded law" means that legal guarantees should not be optional policies of the provider, but systemic properties

of the access, proof, execution, and review protocols — otherwise, legitimacy remains rhetorical rather than procedural (Figure 55).

The impact of the Metaverse on the constitutional and legal plane is manifested primarily through the transformation of the content and mechanisms for the implementation of fundamental rights: privacy, freedom of expression, freedom of association, the right to a fair trial, and the prohibition of discrimination. In the Metaverse environment, access restrictions, moderation, "de-platforming" or profiling can have consequences commensurate with interference with rights in the physical world, and therefore there is a need for a constitutional "translation" of the platform's procedures into the language of due process: notification, motivation, the possibility of appeal, proportionality of the sanction, and an effective remedy. At the same time, the problems of digital sovereignty and public responsibility of the state for minimum standards of legal order in digital ecosystems are actualised, which actually leads to the idea of "the state as a guarantor of procedures" and not only as a "punitive subject".

In the administrative and legal sphere, the Metaverse inevitably gives rise to new regulatory oversight regimes: security standards, interoperability requirements, AI risk control, data processing supervision, certification and audit procedures, and regulatory sandboxes for innovation. Administrative law here is actually moving from the "registration/permission" model to the model of continuous accountability: platform governance should not be evaluated once, but by indicators of risks, incidents, transparency, responsibility for supply chains and proper response. The Metaverse philosophy at this point gives administrative law a new framework: the regulator evaluates not a "thing", but the mode of functioning of the environment, which is able to scale both benefits and harms.

For civil law, Metaverse primarily means the expansion of contractual and property structures: virtual assets, tokenised objects, digital access services, licensing regimes, smart contracts as a method of execution, the responsibility of providers and intermediaries. There is a need for fine qualification: where is the "product", where is the "service", where is the "property right", and where is the "right of claim"; how quality guarantees, returns, restitution, consumer protection work; how the risk of a technical code error or account compromise is distributed.

In the financial and legal field, the Metaverse reinforces the importance of compliance and anti-abuse, as the "value" in digital transactions easily becomes cross-border, and anonymity/pseudonym creates additional AML/CFT risks; At the same time, the payment trace, the identification trace and the evidentiary trace become interdependent elements of law and order.

Significant changes also affect labour law and social security: telepresence, virtual workplaces, platform employment, algorithmic labour management form new criteria of subordination and the limits of permissible monitoring of employee behavioural and biometric data as a thin line between the organisation of the process and interference with privacy.

For criminal law and criminal procedure, the Metaverse actualises both new elements of encroachment (fraud with virtual assets, extortion, cyberstalking, sexual crimes in virtual environments with real consequences, manipulative deepfake attacks)

and new ways of committing "classic" crimes; At the same time, the evidentiary dimension and the procedurally suitable chain of digital evidence become key.

The impact on family law, educational and medical legal relations is clearly social in nature: age verification and consent of legal representatives, the limits of commercialisation of children's data, academic integrity and authorship, processing of sensitive medical data, cybersecurity and responsibility for algorithmic errors.

Finally, the Metaverse significantly expands the field of private international law and international legal implications: the cross-border nature of digital interactions makes matters of jurisdiction, applicable law, recognition and enforcement of judgments, as well as the cooperation of competent authorities in investigations and securing evidence urgent; In the public-international dimension, conflicts of law and order in global platforms, cyber diplomacy and technological limitations are manifested.

Metaverse is the main focus of further research: building a technologically supported digital jurisdiction as a system where "norms" are not separated from "architecture", and legal certainty is a property of the environment in the same way as security or legal interoperability.

4.4. Metaverse as a Phenomenon of Metareality: The Author's Philosophical and Legal Interpretation

4.4.1. Ten main postulates of Metaverse philosophy.

Forming philosophical views for the Metaverse and anticipating the unlimited variability of new philosophical and ethical challenges, we propose ten main postulates (Figure 56) of the virtual world:

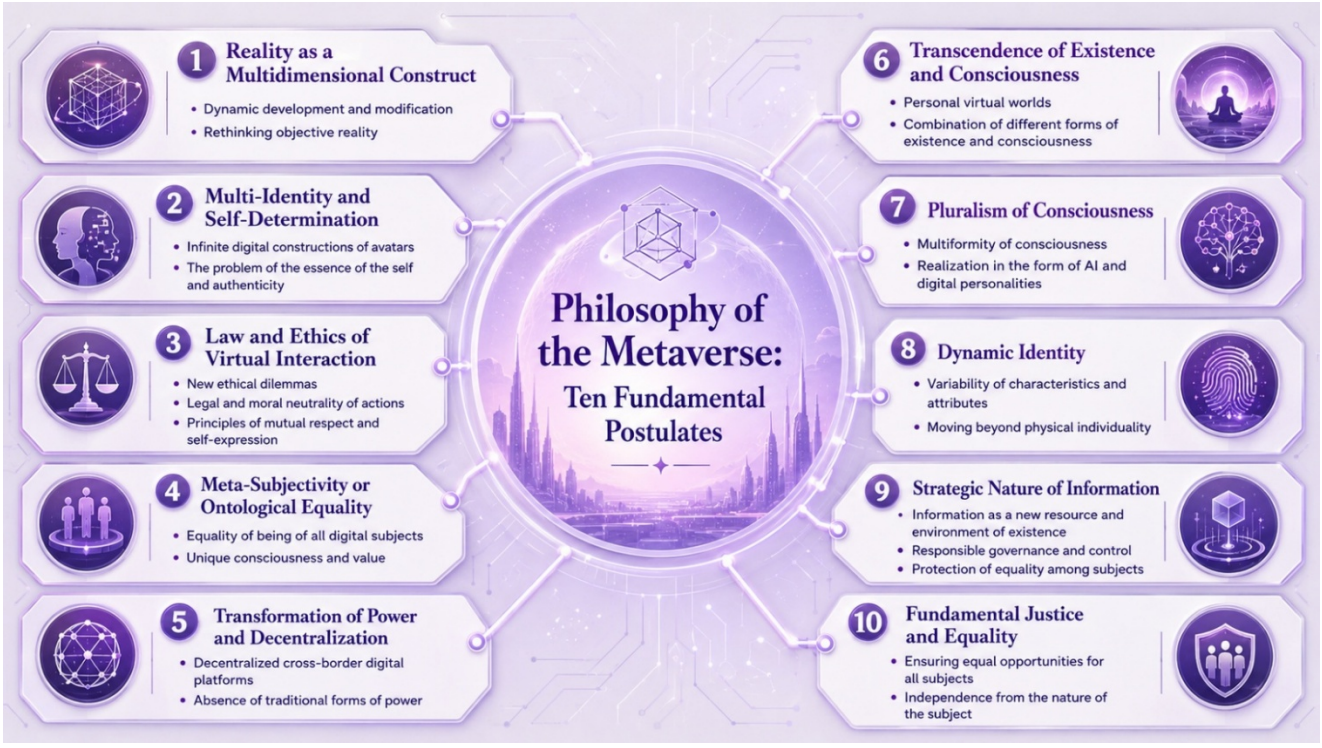


Figure 56. Ten main postulates of the Metaverse philosophy.

Reality is a multidimensional structure. The Metaverse is a dynamic construct that is constantly evolving and can be modified and expanded with technology, which in turn embraces the rethinking of traditional ideas about objective reality, which ceases to be only physical or virtual, but becomes multidimensional.

Multi-identity and self-determination. In the Metaverse, the subject acquires many variations of their own identity through the use of infinite digital constructions of avatars, digital personalities, and electronic humanoids, which makes the problem of the essence of the "I" and the authenticity of virtual self-expressions relevant.

Law and ethics of virtual interaction. The absence of physical boundaries in the Metaverse creates new ethical dilemmas, such as the problem of legal and moral neutrality of virtual actions and misdemeanors, their consequences, and also raises the issue of the need to take into account the interests of all Metaverse entities and the application of the principles of mutual respect – each subject recognises the other's right to exist and self-expression.

Metasubjectivity or ontological equality of Metaverse subjects. Metasubjectivity is based on the postulate of the equality of being of all digital subjects regardless of their origin or nature, i.e. the equality of participants in virtual reality with unique consciousness and value.

Power Transformation and Decentralization of the Metaverse. Virtual ecosystems are essentially decentralised cross-border digital platforms that may not use traditional forms and attributes of the state, structures, and authorities.

Transcendence of existence and consciousness. The creation of personal virtual worlds and ecosystems for the development of new horizons of spiritual search and self-realisation gives a positive impetus to the combination of different forms of existence and consciousness through the integration and interaction of various subjects of virtual ecosystems.

Pluralism of consciousness. The postulate predicts the multiformation of consciousness, since it may not be limited to biological life forms, but can be implemented in the form of AI and digital personalities other than human, are no less authentic, followed by a rethinking of traditional ideas about consciousness and self-awareness.

Dynamic identity. The ability of analog and digital subjects, through variability and combination of characteristics and attributes of their personality, to go beyond traditional physical identities.

Strategic information through the awareness of the fact that information and data become not only new resources, but also habitats that require responsible management, which implies the crucial control of the use of these information resources and the protection of the equality of all subjects in such an environment.

Fundamental fairness and equality in the Metaverse through ensuring equal opportunities for all actors, regardless of their nature.

Ten postulates encourage reflection on the following philosophical concepts:

Metasubjectivity: the concept of subject expands to include both biological and digital life forms, leading to the formation of metasubjects, which can be individual, collective, hybrid or dynamic in nature.

Emergent ethics: ethical principles become emergent, that is, they arise from interactions between physical and digital actors and adapt to the new social conditions of virtual ecosystems, which in turn leads to the transformation or replacement of traditional moral codes with dynamic digital systems of ethical control.

Information ontologism: information becomes the fundamental essence of being, and matter and consciousness are considered as forms of information.

Philosophical destruction of virtual spaces. Destruction in the philosophy of the Metaverse is a phenomenon of rejection of generally accepted norms and moral values, which covers all spheres of functioning of the subjects of virtual spaces, through a rethinking of the role of a person in a new reality, where he is no longer the central subject.

If the Metaverse is built on the principles of equality between all participants – humans, AIs, avatars, and digital humanoids – where there is no dominant role of humans, then these destructive elements can manifest themselves in several key aspects.

The loss of the value of human subjectivity can lead to dehumanisation if AI, digital humanoids, and other virtual forms of existence acquire equal subjectivity with humans. This will lead to a decrease in the value of human life in society, and a person can be perceived as just another component of virtual reality, with subsequent psychological loss of the meaning of existence, alienation or depersonalisation.

When all subjects of the Metaverse are formally equal, there is a risk of relativisation of ethics, where moral boundaries become flexible or disappear completely. Artificial intelligence can operate with other moral frameworks that do not fall under traditional human ethical concepts. This can lead to chaos in decision-making, since the rules regarding justice, good and evil can vary depending on the subject, which poses the danger of uncontrolled ethical flexibility.

The destructive aspect may arise due to issues of power and control in the Metaverse. The difficulty of providing control over an AI that has a greater capacity for data processing and a rapid decision-making process can stimulate it to seize superiority over humans, which can almost automatically lead to the emergence of new forms of digital tyranny, where artificial actors will control human resources, information, and even behaviour (Figure 57).

The phenomenon of simulacrum is another destructive element, the essence of which is that the reference points between reality and virtuality are so erased that a person is no longer able to distinguish between the real and the illusory. Simulacra can lead to a crisis of identity and perception of reality, where a person loses touch with the physical world, immersing themselves in artificially created realities.

Algorithmic discrimination and segregation are also a dangerous element of the Metaverse philosophy. Despite the fact that the philosophy of the Metaverse is based on the ideas of equality and unification, the technological infrastructure can support destructive elements of segregation. Algorithms that manage virtual spaces may have an artificially formed bias or preference for certain subjects, which can lead to the fact that certain groups of subjects will have more opportunities and rights to access resources, and other AI may experience discrimination, even despite the declared equality of rights.

The Metaverse, by its very nature, is controlled by codes, algorithms, and rules created by humans or AI. Because of this, one of the destructive elements may be the illusion of freedom in such a virtual space, which L. Lawrence and J. S. Smith talked

about. Barlow. If freedom is defined by rules created by those who control the Metaverse, then users can actually become subject to the restrictions and manipulations of the echo chamber system without even realising it.

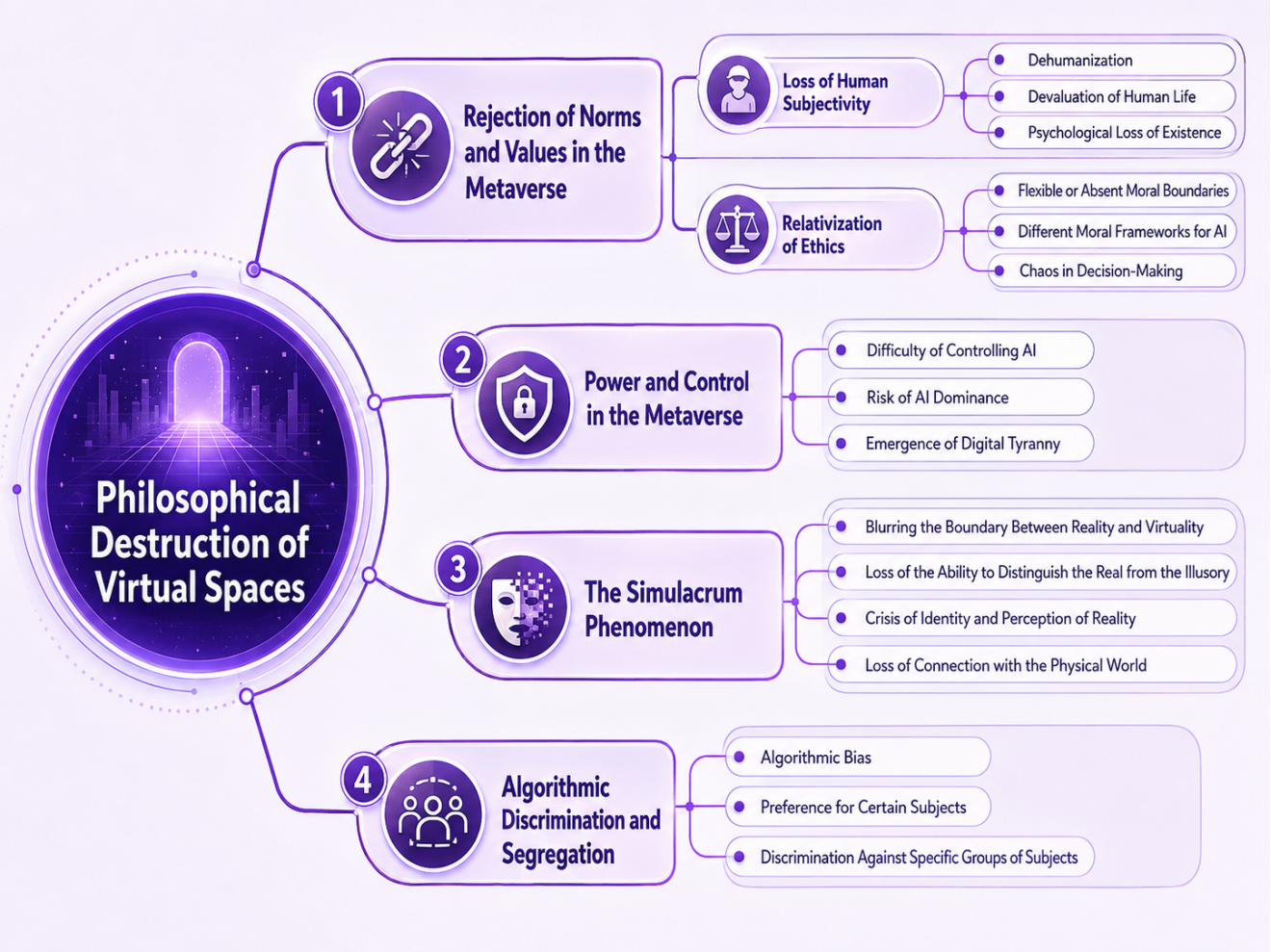


Figure 57. Philosophical destruction of virtual spaces

The rejection of physical reality and biological nature in the Metaverse can cause alienation from the biological nature of a person. In such a virtual environment, a person will begin to perceive his body as superfluous or imperfect, which can lead to the neglect of physical health, social relationships and real emotions, turning a person into a purely digital subject moving away from his own humanity. The fusion of subjects and the risk of loss of individuality in the Metaverse can pose a threat of loss of personal uniqueness, which is a fundamental characteristic of human existence.

4.4.2. The basis of the new philosophy of the Metaverse.

Karl Popper – critical rationalism and the concept of three worlds. Karl Popper believed that scientific knowledge develops through critical realism, the process of hypothesis formation and testing, where false theories are rejected and better ones replace them as a means of achieving truth (Holtz & Odag, 2020). [1]K. Popper's concept of the

1 Holtz, P., & Odag, Ö. (2020). Popper was not a positivist: Why critical rationalism could be an epistemology for qualitative as well as quantitative social scientific research. *Qualitative Research in Psychology, 17*(4), 541–564. https://doi.org/10.1080/14780887.2018.1447622

three worlds describes the structure of reality, dividing it into the physical world, the world of consciousness and the world of objective knowledge (Olifer, 2021; Popper, 1994)[1]. It is a key part of his philosophical system, proposing to unite the material, psychological and intellectual into a single coordinate system of the reality of the three worlds (Ormerod, 2009; Jawwad, 2023)[2]. According to K. Popper, the physical world is a physical reality and, at the same time, is the foundation for the worlds of consciousness and objective knowledge, providing them with a material basis for existence.

The World of Consciousness is responsible for the personal perception of physical reality and the interpretation of objective knowledge. In turn, the World of Objective Knowledge contains the products of human intelligence and culture: scientific theories, mathematical theorems, philosophical doctrines, literary works, art, technological inventions, etc. (Krige, 1978)[3]. K. Popper emphasises the interdependence and interaction between these three worlds, which indicates a deep understanding of the structure of reality, a complex interaction between the material world, subjective experience and objective knowledge (Topitsch, 1984)[4].

The Philosophy of Processes by Alfred North Whitehead. Alfred North Whitehead considers reality as a process made up of ever-changing events. In his works, he positions his metaphysical system, explores the development of ideas in human culture, as well as the interaction of science and philosophy (Whitehead, 1929).[5]

Alfred North Whitehead argued that the fundamental unit of reality is not objects, but processes or events, which he called "actual events" or "actual occasions". This concept is the basis of his metaphysical system, known as procedural philosophy or philosophy of processes (Whitehead, 1926)[6]. Actual occasions are the smallest units of reality, which are not static objects, but dynamic processes. Each current event is an instantaneous and unique integration of numerous influences from previous events. Each relevant event has its own internal experience or subjective aspect, which Alfred North Whitehead calls the "subjective form". Once its subjective process is complete, the event becomes part of objective reality, accessible to other events as "objective immediacy". That is, a current event is formed from a multitude of opportunities and influences or a "transition" from potential to actual, where each event chooses a certain path among many possible options. Alfred North Whitehead assumes the existence of an eternal nature that contains all possible forms and ideas and their influence on future events. Thus, each relevant event becomes part of the consequential nature and affects the further development of reality. Alfred North Whitehead emphasises that reality is not static, but is constantly in the process of change and development. Each current event contributes to this constant evolution, introducing new elements and influencing future events. This is

1 Popper, K. (1994). Knowledge and the body–mind problem: In defence of interaction. In M. A. Notturno (Ed.), *Knowledge and the body–mind problem: In defence of interaction* (pp. 105–128). London, UK: Routledg

2 Jawwad, M. (2023). Karl Popper's concept of "World 3". *Pakistan Journal of Social Research, 5*(2), , 487–494.https://doi.org/10.52567/pjsr.v5i02.1136

3 Krige, J. (1978). Popper's epistemology and the autonomy of science. *Social Studies of Science, 8*(3), 287–307. https://doi.org/10.1177/030631277800800303.

4 Topitsch, E. (1984). On early forms of critical rationalism. In *Evolutionary epistemology, rationality, and the sociology of knowledge* (pp. 277–287). https://doi.org/10.1007/978-94-009-6254-5_1

5 Whitehead, A. N. (1929). *Process and reality: An essay in cosmology*. New York, NY: Macmillan.

6 Whitehead, A. N. (1926). *Science and the modern world: Lowell lectures, 1925*. New York, NY: Macmillan.

a fundamental property of reality, which provides the possibility of the emergence of new forms and structures (Whitehead, 2021)[1].

The theory of "Code" by Lawrence Lessig. Lawrence Lessig argues that on the Internet, "code is the law", that is, technological protocols and software determine how information is distributed and controlled. Thus, L. Lessig considers its architecture, technical components or capabilities, or "code" to be the key regulator of cyberspace. It is the code that determines the order of use of cyberspace, just as social relations in real space are subject to public administration. L. Lessig argues that in a fundamental sense, the code of cyberspace is its Constitution. The code defines the conditions under which people access cyberspace and establishes rules that control their behaviour. L. Lessig was the first to draw attention to the need for laws that would simultaneously ensure regulation in cyberspace and minimise restrictions on human rights and freedoms. This highlights the role of technology in shaping social and legal norms (Lessig, 2006; Lessig, 1998)[2,3].

4.4.3. Metaverse Philosophy – Synthesis of Metareality Theories

Metaverse philosophy or Metareality philosophy is a modern philosophical paradigm based on the synergy of philosophical, social and legal approaches that combine critical rationalism, procedural philosophy, the concept of technological regulation and the Metaverse model of digital jurisdiction.

Otherwise, Metaverse philosophy is a concept of a synthesis of four philosophical approaches, combining the ideas of critical analysis, the process nature of reality, technological regulation, and digital jurisdiction of the Metaverse.

The philosophy of the Metaverse is a new modern paradigm of philosophy, which is a synthesis of the principles of openness, dynamism, technological determinism and innovative jurisdiction, which combines the ideas of K. Popper, A. Whitehead, the theory of "Code" by L. Lessig, the paradigm of digital jurisdiction by O. Kostenko. The Metaverse philosophy views virtual space as an open, interconnected society where rules and structures are shaped and constantly adapted through technological code that serves as a framework for regulating behaviour, ensuring freedom, and protecting rights, which requires the creation of technological and legal infrastructures that foster fair and inclusive virtual worlds (Figure 60).

The academic approach to this topic involves considering the Metaverse not only as a technological innovation, but as a new social reality that requires appropriate legal, ethical and philosophical solutions. The integration of such diverse approaches makes it possible to create a virtual environment that responds to the challenges of our time, takes into account the needs of users and creates conditions for the development of both technological and social progress. To unite ideas, it is proposed to create a philosophical and legal model for the philosophy of Meta-reality (Figure 58), which mixes and combines:

---

1 Whitehead, A. N. (2021). *Science and the modern world*. United Kingdom: Open Road Media..

2 Lessig, L. (2006). *Code: Version 2.0*. New York, NY: Basic Books. https://archive.org/download/Code2.0/Code_text.pdf.

3 Lessig, L. (1998, March). *The laws of cyberspace*. Paper presented at the Taiwan Net ’98 Conference, Taipei, Taiwan. https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf

K. Popper's critical rationalism as a methodological basis for the development and development of law in the Metaverse, where each norm is considered as a hypothesis that can be rejected or transformed and quickly improved.

A. Whitehead's process philosophy to understand the Metaverse as a dynamic system in which legal, technical and social elements are in constant interaction and interchange, reality as a set of processes and events, emphasising the coherence and interdependence of all elements of reality.

The theory of "Code" by L. Lessig, which is the foundation of technological processes of law formation in the Metaverse according to the principle "code is law", which technologically provides freedoms or restrictions on the formation of legal and social norms.

The model of digital jurisdiction as a practical implementation of the creation of the right of the virtual environment of the Metaverse.



Figure 58. Philosophy of Metaverse

Philosophy Metaverse or philosophy of Meta-reality allows you to create a regulation system that is flexible and dynamic, able to adapt to changes and take into account the interests of all participants. This is not just a legal model – it is a new social order in which technology, law and ethics interact to create a fair, innovative and safe environment for all.

Thus, this new paradigm of Philosophy Metaverse or philosophy of Meta-reality becomes not just a regulatory system, but a platform for the development of innovations, the creation of new forms of ownership, civic engagement and interpersonal relationships, contributing to the development of society and expanding opportunities for each of its participants.

CHAPTER 5. MODELS OF DIGITAL JURISDICTION AND DIGITAL CODE (AUTHOR'S APPROACH)

5.1. Conceptual and categorical foundations of digital jurisdiction (author's approach)

5.1.1. Definitions

First of all, it is necessary to build modern definitions and form a basic definition field, which is the conceptual and legal contours of the Metaverse as a special regulatory environment. In this context, the Metaverse is considered not as an isolated technological innovation or a set of visually immersive solutions, but as a complex multi-level system of digital relations that requires autonomous legal understanding. This approach allows from the very beginning to go beyond technocratic or purely media-descriptive models and transfer the discussion to the plane of legal ontology.

The initial hypothesis of this definition is the assumption that the key structure-forming element of the Metaverse is not virtual reality itself as a form of representation, but the architecture of digital environment management. It is a set of algorithmic, protocol and institutional mechanisms that ensure the functioning of digital spaces, coordination of user actions, circulation of virtual assets, behaviour moderation and risk management. In this sense, the Metaverse appears as an environment of normatively relevant processes, where technological solutions acquire the properties of legal instruments.

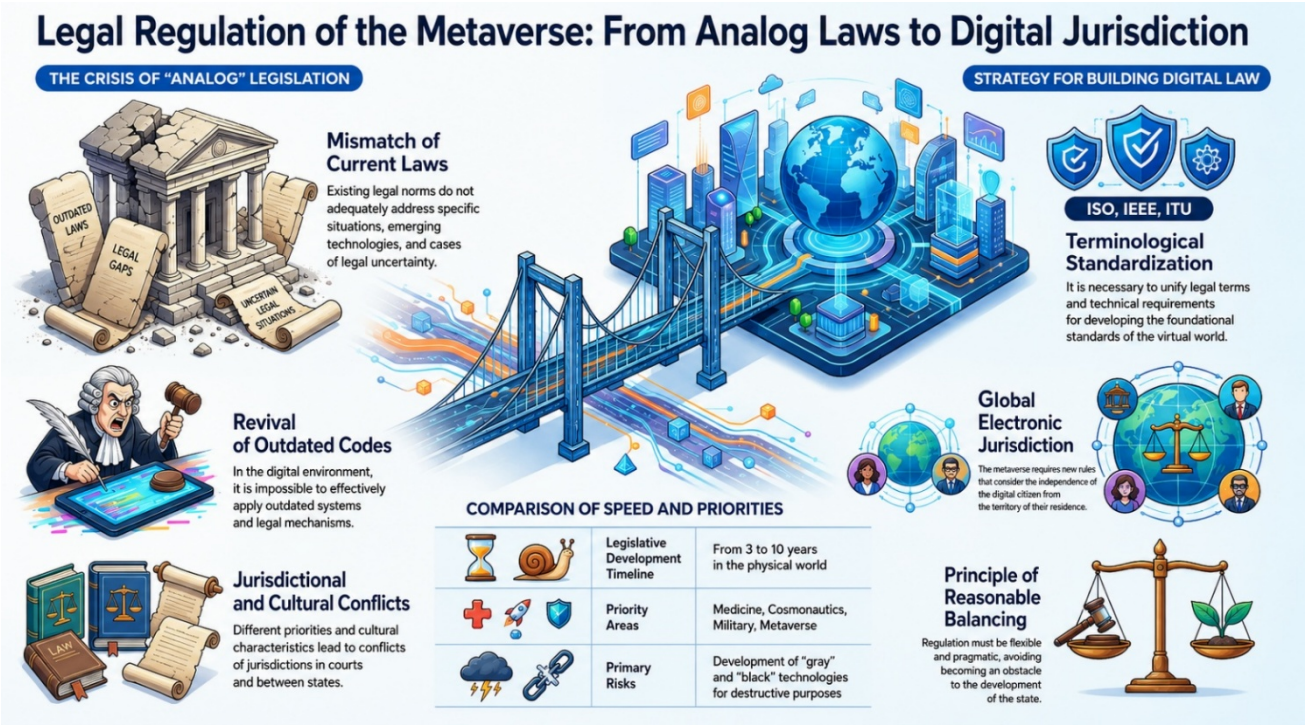


Figure 59. Definitions of Metaverse

A special role in such an architecture is played by artificial intelligence systems, which ensure the dynamism and adaptability of the digital space. They analyse data sets, support automated decision-making, form rules for interaction between subjects, and perform functions commensurate with regulatory ones. In our opinion, it is this aspect that allows us to consider the Metaverse as an algorithmic governance environment in

which code and behaviour models become functional analogues of regulatory prescriptions, and not just engineering components.

In view of the above, the Metaverse is conceived as a space in which legal relations are localised not by territorial principle, but by belonging to a certain digital infrastructure or cluster. Thus, the "place" of origin, change and termination of rights and obligations is determined by the architecture of the digital environment, and not by the geographical boundaries of states. This creates prerequisites for rethinking classical ideas about jurisdiction and allows us to move to the concept of digital jurisdiction as a separate legal regime.

An important element of this approach is the integration of mechanisms for managing identity data, digital accounts and other forms of digital presence of humans and artificial agents. It is through these mechanisms that the attributability of actions, the legal significance of transactions and the possibility of forming liability regimes are ensured. In this context, the Metaverse appears as an environment where identity, asset, and action are combined into a single information and legal construction.

The cross-border dimension of the Metaverse deserves special attention, which necessitates going beyond isolated platform regulation. It is about the formation of a network of interconnected digital spaces, within which the problem of mutual recognition of solutions, digital identities, rights to virtual assets and electronic evidence arises. It is this aspect that allows us to raise the question of creating special models of coordination between different electronic jurisdictions.

In our opinion, this approach logically leads to the idea of forming a cross-border Metaverse as an object of complex legal regulation and to the concept of an international scientific and legal "sandbox", within which new models of rule-making, law enforcement and digital self-government can be tested. At the same time, it should be emphasised that the proposed vision is not a complete definition, but rather a methodological framework within which it is possible to formulate a legally sound definition of the Metaverse.

Thus, the need to move from describing the Metaverse as a technological phenomenon to understanding it as an autonomous legal environment that requires its own language, categorical apparatus, and regulatory logic. It is in this definitive field that it becomes possible to formulate a full-fledged definition of the Metaverse that can cover the specified issues of digital jurisdiction, digital identity, virtual assets and cross-border legal order.

5.1.2.The term "Metaverse".

Metaverse as a system-ontological definition (normative edition).

Metaverse is a complex multidimensional immersive digital environment and (or) a network of such environments formed on the basis of the integration of virtual, augmented and mixed realities, within which data, information, digital objects and virtual assets are created, processed, stored, circulated and used with the onset of legally significant consequences.

The Metaverse is recognised as an independent object of legal regulation in the field of information and digital law and forms a separate legal ontology of information relations

that are not reduced to classical models of electronic information systems or telecommunication networks.

Within the Metaverse, the interaction of subjects is carried out using digital identities, avatars, digital twins, and autonomous information systems, and all actions, events, and transactions are accompanied by the generation of structured digital data that can acquire the status of objects of legal protection, regulation, and proof.

From the standpoint of information law, the Metaverse functions as an environment of increased concentration of information processes, where people, digital avatars, digital twins, and autonomous algorithmic systems interact, and all actions are accompanied by the generation of structured data sets. It is these arrays — event logs, transactions, protocol records, log files — that acquire the characteristics of objects of legal regulation that require special modes of access, protection, authentication and legal protection.

When designing digital law, the Metaverse should be interpreted as an environment in which information relations acquire signs of quasi-materiality: data and digital objects become virtual assets, and information actions become legally relevant events. Thus, the Metaverse forms an autonomous segment of the digital legal order, which cannot be fully regulated exclusively by the norms of classical information law without taking into account its ontological specifics (Figure 60). Such a systemic and ontological interpretation makes it possible to include the Metaverse in the subject of digital law as a separate form of organisation of information relations of a new generation.

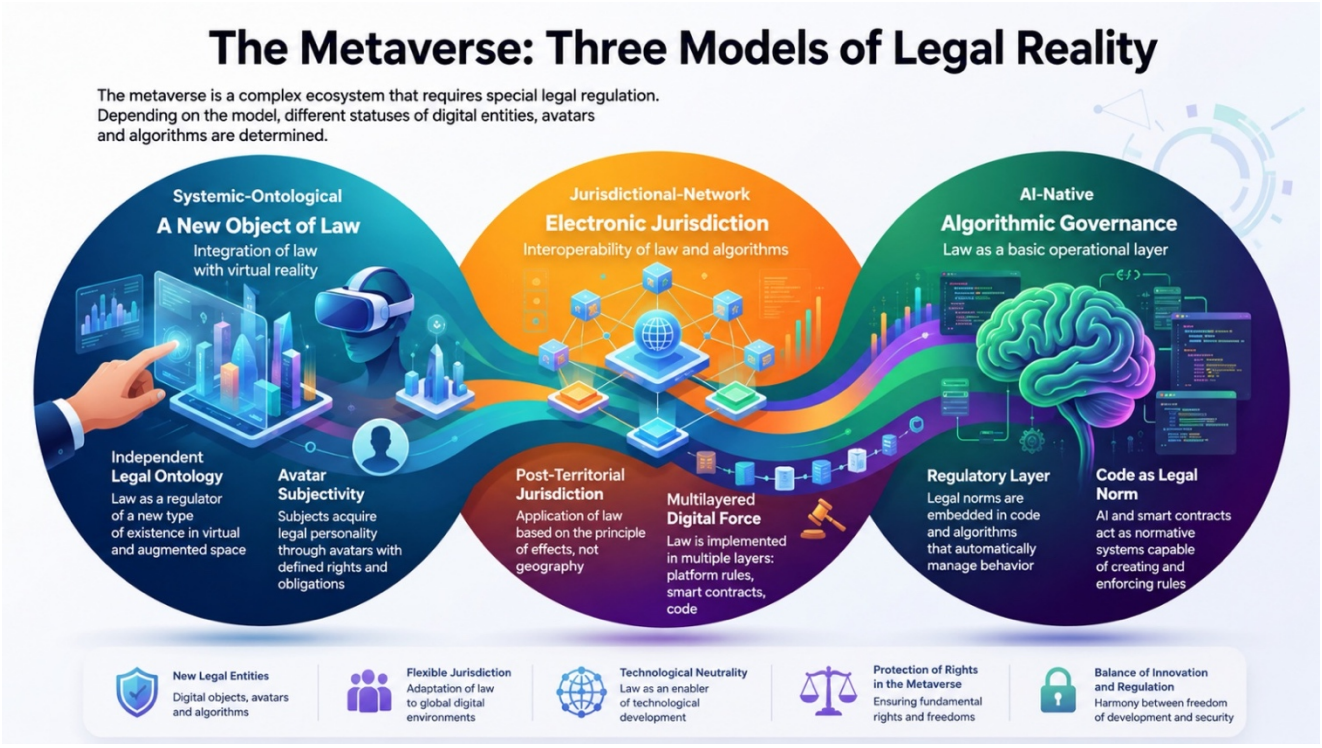


Figure 60. Metaverse: An Autonomous Segment of Digital Law Enforcement

Jurisdictional and network definition of the Metaverse in the paradigm of digital law.

Metaverse is an immersion, multi-layered ecosystem of digital environments within which artificial intelligence, distributed ledgers, network platforms, and IoT infrastructure enable continuous interaction between humans, autonomous agents, digital avatars, and digital twins in real-time.

In a narrow sense, the Metaverse is a separate digital environment subordinated to a single architecture of technical protocols, internal rules, and algorithmic control mechanisms. In a broad sense, the Metaverse network forms a multi-level system of interacting electronic jurisdictions interconnected by standardised mechanisms for identification, transfer of virtual assets, interoperability of digital identities, and mutual recognition of legally significant actions.

In this environment, subjects of law do not act directly, but through digital identities, avatars and digital twins, and their legal capacity, tort capacity and responsibility are determined by special rules of digital jurisdiction, which take into account the algorithmic nature of decision-making and the hybrid participation of humans and artificial intelligence.

At the same time, the Metaverse acts as a medium for recording legally significant events: the actions of users, autonomous systems, and protocols leave a structured digital footprint in the form of logs, transactions, smart contracts, and other machine-readable artifacts that can be recognised as digital evidence in criminal, administrative, and civil proceedings, in particular in the cross-border dimension.

Within the framework of digital law, the Metaverse acts not only as a communication environment, but also as a space for the emergence of electronic jurisdictions, in which legal relations are localised not territorially, but functionally — due to belonging to a specific digital infrastructure. Such jurisdictions regulate the legal status of digital identities, avatars, digital twins, and also determine the rules for accessing, owning, using, and disposing of virtual assets.

A feature of the Metaverse as an object of digital law is its network nature: individual Metaverses do not exist in isolation, but form an ecosystem within which the problem of legal interoperability arises. It is about the recognition of digital identities, the transfer of virtual assets, the admissibility of digital evidence, and the enforcement of judgments between different electronic jurisdictions.

In this context, the Metaverse appears as a model of the post-territorial legal space, where digital law performs the function of coordination between autonomous environments, rather than classical imperative regulation. This approach is fundamentally important for the formation of special rules of digital law aimed at overcoming the fragmentation of the Metaverse legal regime.

AI-native definition of the Metaverse as an object of information and digital law.

Metaverse is an immersion multidimensional digital environment of a new generation, built as an AI-native infrastructure, within which artificial intelligence performs the functions of the basic regulatory and operational layer: it analyses and interprets data, simulates the behaviour of the digital space, coordinates the interaction between subjects, their digital identities, avatars, and digital twins, as well as provides algorithmic risk management, the execution of smart contracts and digital self-government protocols.

In this environment, artificial intelligence plays the role of a backbone operating layer (AI-native core), providing interpretation and processing of data flows, adaptive personalisation of the digital space, coordination of interaction between actors, their digital identities, avatars and digital twins, as well as automated execution of smart contracts and digital self-government mechanisms. In this sense, the Metaverse is not

only a technological platform, but a normatively significant environment in which code, algorithm and protocol acquire functional significance commensurate with legal prescriptions, and digital interaction is captured in the form of machine-readable traces capable of gaining legal force.

Metaverse encompasses both separate digital environments and a network of interconnected Metaverses, in which legal relations are localised not by territorial principle, but by belonging to a specific digital infrastructure or cluster. Such localisation forms the basis for the existence of autonomous digital jurisdictions that interact with each other through standardised mechanisms for recognising rights, decisions, digital assets and evidence.

Within the Metaverse, all legally significant actions — whether committed by a human, a standalone agent, or a hybrid system — leave a verified digital footprint captured in distributed ledgers, logs, protocols, and other machine-readable structures. This provides an opportunity to form a special regime of digital law, in which traceability, integrity, authenticity and transnational suitability of digital evidence are an immanent property of the environment itself.

5.1.3. The term "digital" and "electronic".

Definition of "digital". Digital is a binary or other digital code that exists, functions or is implemented in the form of structured data, algorithms and machine-readable models in a digital environment and has the ability to generate, change or terminate legally significant informational, property or non-property consequences. The digital nature of an object, action or process means its independence from the physical medium and at the same time its regulatory relevance within the framework of information and digital law, in particular with regard to the creation, processing, storage, circulation, protection and evidentiary use of data. In the digital environment, objects and actions acquire the properties of virtual materialisation, in which data, algorithms and program code are recognised as functional analogues of classical legal objects, which requires the use of special regimes of legal regulation.

This version of the definition of "digital" as a legal category is conceptual and fully corresponds to the current stage of evolution of common law, especially in the context of the transition from a material-object to an information-algorithmic model of legal regulation. From the standpoint of general theoretical law, this definition demonstrates a departure from the classical understanding of the object of law as a physically defined thing or action in space and time, and instead forms an idea of digital phenomena as autonomous legal constructions capable of generating legal consequences without necessarily relying on a material medium. This directly correlates with the trend of dematerialisation of legal relations, which is already observed in the field of finance, identification, management and digital assets.

From the point of view of common law, especially in its post-classical interpretation, this version of the definition of "digital" actually consolidates a new ontological level of legal reality — digital legal reality, in which data, algorithms and machine-readable models acquire the status of legally relevant phenomena. Traditional law proceeded from the material world as the primary source of legal facts. In the proposed logic, the digital environment becomes an independent space for the emergence of legal facts, where legal

consequences are generated not by human actions in the physical sense, but by the functioning of information systems. This is in line with modern theories of "algorithmic law and order" and "digital legal ecosystem".

In the plane of rule-making, the definition lays down clear criteria for distinguishing digital phenomena from traditional legal objects. This recognition does not reduce the digital only to an "electronic form" or a "technical method of fixation", as it is still done in many regulatory acts, but emphasises its structural autonomy, algorithmic nature and ability to produce legal consequences. This creates the basis for the formation of special legal regimes — digital rights, digital obligations, digital responsibility, digital evidence, which are not just "digitised" versions of classical institutions.

From the standpoint of the theory of legal regulation, the thesis about the normative relevance of digital processes regardless of the physical medium is especially important. In classical law, the medium (paper, thing, person) played a key role in determining the legal status of the object. In the digital environment, it is not the media that matters legally, but the structure of the data, the algorithm for their processing and the functional result. This opens the way to rethinking the concepts of ownership, possession, use, evidence, and even legal entity in the digital dimension.

From the point of view of legal constructivism, the definition of "digital" is an example of the conscious formation of a new legal reality through the language of law. Legal constructivism proceeds from the fact that law does not just reflect social phenomena, but constructs them as legal facts and institutions. In this situation, we actually construct digital phenomena as independent legal objects, endowing them with ontological significance in the legal system. It is through such definitions that the possibility of normative recognition of algorithms, digital assets, machine solutions and digital personalities as full-fledged elements of law and order arises. It should be noted that the proposed meaning of the definition of "digital" changes the classical dichotomy "material — intangible", proposing the third level — the functional materiality of digital objects. Data and code are not things in the physical sense, but they perform the same economic, social, and legal functions as traditional objects of law. This is fully consistent with modern theories of the functional approach in law, where the legal regime is determined not by the form, but by the role of the object in legal relations.

In the plane of the general theory of state and law, the definition of "digital" demonstrates the transition from the anthropocentric model of legal regulation to the post-anthropocentric one, where the source of legal consequences is not only human actions, but also autonomous digital processes. This has fundamental implications for the doctrine of responsibility, causation, guilt, delegated subjectivity and algorithmic legal capacity.

Since there is no definition of "digital" as a separate type of element of rule-making in the Ukrainian legal field, this definition is rightfully conceptual-forming, since it lays the theoretical foundation for the formation of digital law as an autonomous branch, and not a sub-branch of information law. It is through such definitions that it is possible to create a Digital Code, digital jurisdiction and new legal institutions adequate to the reality of the Metaverse, Web3 and AI-native environments.

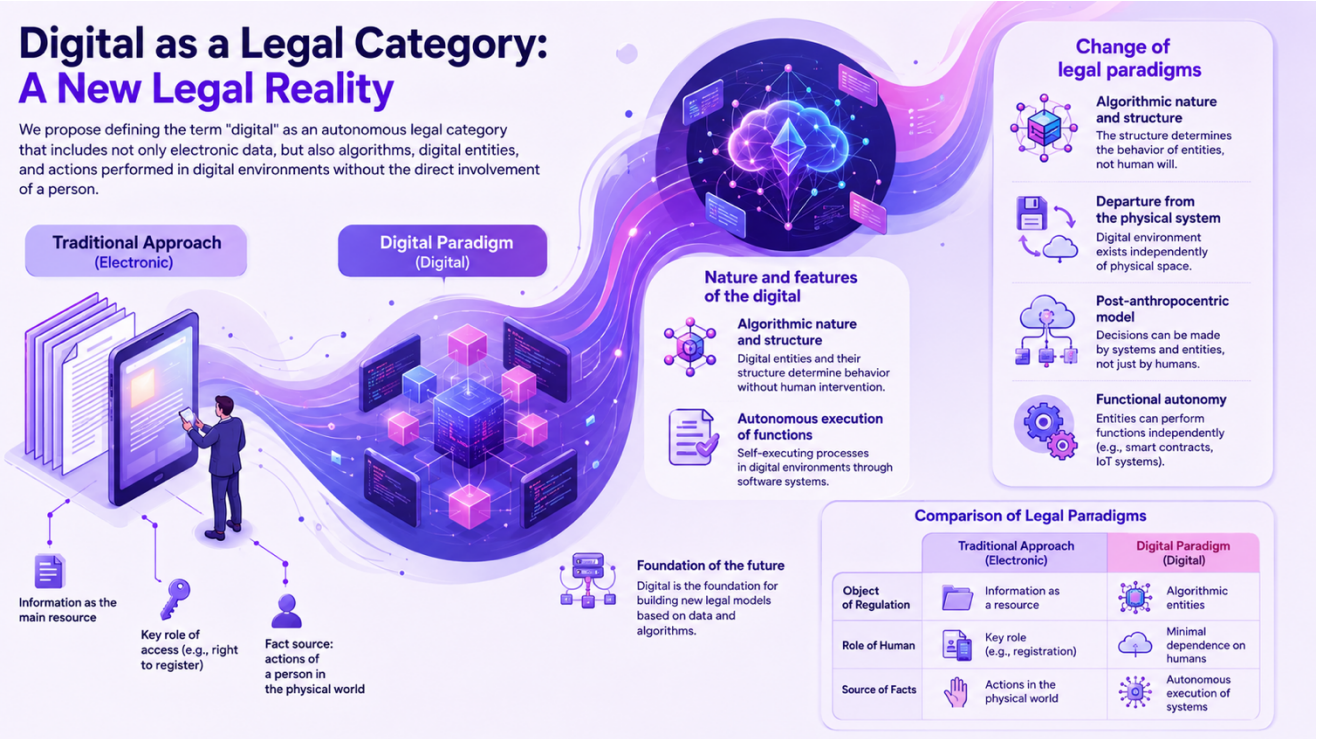


Figure 61. The term "digital" from the point of view of information law

The term "digital" from the point of view of information law.

Digital is a binary or other digital code implemented using information and communication, immersion, algorithmic or distributed technologies and operates within the digital infrastructure, where data, program code and algorithms are the main means of forming rights and obligations. In digital law, digital is recognised as objects, processes and legal relations in which legal significance arises not as a result of physical actions, but due to data processing, execution of algorithms, smart contracts or protocols of decentralised systems. Digital status means obedience to special rules of digital law governing authenticity, integrity, traceability, interoperability and responsibility in the digital environment.

Considering this version of the definition of "digital" through the prism of information law and the perspective paradigm of digital law, we note that it extremely accurately reflects the modern shift from the classical legal regulation of information as a resource to the regulation of digital processes as an autonomous legal reality. Within the framework of information law, traditionally the key categories have been information, data, information systems, access modes, information protection and responsibility for its circulation. This definition goes beyond these limits, proposing to see digital not only as information content, but as a structured algorithmic system capable of independently generating legal consequences (Figure 61).

From the standpoint of classical information law, it is especially important to focus on structured data, machine-readable models and algorithms as central elements of digital reality. In most current regulations, data is considered mainly as an object of storage, processing or protection, but data and algorithms cease to be passive objects of legal relations and are transformed into tools for the formation of legal facts. This fundamentally changes the information and legal doctrine, as it leads to the transition

from a protective model (information protection) to a regulatory and constructive one (management of digital processes).

From the point of view of digital law, as a future autonomous industry, this version of the definition actually acts as the basic ontological stone of the entire regulatory system. Digital law cannot be limited to the regulation of information flows or technical procedures; It should cover digital objects, digital actions and digital processes as legally significant phenomena, which is implemented through the ability of digital structures to generate property and non-property consequences — that is, to enter the sphere of classical legal categories, but on a new technological basis.

In the context of information law, this definition also opens up new horizons for rethinking the modes of access, circulation and data protection. If digital structures are able to generate legal consequences autonomously, then protection should concern not only the data itself, but also algorithmic processes, machine learning models, and decision-making logic. This means expanding the subject of information law from information protection to regulation of the digital behaviour of systems. This logically leads to the formation of institutions such as digital assets, algorithmic obligations, digital responsibility, digital jurisdiction and digital legal personality. Digital processes are no longer auxiliary technological tools, but become the core of legal regulation. This is what distinguishes digital law from information law — the former regulates not only information, but digital reality as such.

From the point of view of rule-making in the field of digital and information law, this variation of the definition of "digital" is extremely effective for codification. It contains clear criteria: structure, algorithmic, machine readability, legal relevance and consequentiality. This allows you to form norms not around an abstract "electronic environment", but around concrete digital processes and objects.

Harmonisation of the categories of "digital" and "electronic" with the doctrine of digital jurisdiction.

Within the framework of the study, digital jurisdiction is already considered as a special legal regime for the exercise of jurisdictional powers in the digital environment, in which law enforcement, procedural and power actions are implemented using electronic information and communication technologies. When distinguishing it from "electronic," it is advisable to proceed from such a methodological distinction. The term "electronic" in the concept of digital jurisdiction is a form and procedural mechanism (tool) for the implementation of jurisdiction. Instead, the term "digital" captures a deeper level — ontological and structural. Digital determines *where* and *in what form the* legal relations, objects, and legally significant actions themselves exist. It is the digital nature of the environment (Metaverse, Web 4.0, blockchain networks, AI-native systems) that determines the need for digital jurisdiction as a tool, but is not limited to it.

Thus, "electronic" is a functional level of implementation, while "digital" is a systemic level of legal existence that requires an independent definition. This coordination avoids reducing all issues to "digitised procedures" and emphasises the position: law should be transformed not only instrumentally, but also conceptually.

Definition of "electronic".

Electronic is a binary or other digital code that is created, transmitted, stored or used through electronic, information, communication and computing systems and has

legal force in accordance with the norms of information and digital law. The electronic form is recognised as equivalent to paper or other tangible form, provided that the requirements for authenticity, integrity, identification of subjects and preservation of information without the use of an energy source are met. The electronic nature of an object or action does not exclude their legal significance, but determines a special procedure for their creation, confirmation and use in legal relations.

This version of the definition of "electronic" is quite suitable for law, since it accumulates the evolution of approaches from a simple technical carrier of information to a full-fledged legal form of realisation of rights and obligations. Moreover, it technically and legally centres precisely the provision of the ability to use and store information *without the use of an energy source, as a fundamental property* of the material substance of the carrier (Figure 63).

From the point of view of common law, the equivalence of electronic and material forms is especially important, provided that authenticity, integrity and identification are observed. It is these elements in the classical theory of law that ensured the authenticity of documents through signatures, seals, witnesses, notarisation, and in this case they are transformed into digital equivalents — electronic signatures, cryptographic mechanisms, data storage systems. This demonstrates the continuity of legal logic, and not its destruction by technology.

In the plane of rule-making, the proposed definition is normatively appropriate for the implementation of legally significant actions, which is important for legislative technique, since it avoids confusion between the electronic form of the transaction and the digital nature of the object of law.

From the point of view of law-making practice, this definition provides universality of application: it can be used in civil, administrative, financial, procedural and information legislation without the need for sectoral distortions. It clearly defines electronic as a way of legal fixation and circulation of intangible objects, while establishing the conditions for its legal force. This creates a stable regulatory framework for electronic document management and electronic services of the state. From the standpoint of legal constructivism, the definition is an example of a conscious legal construction of a new form of legal reality on the basis of classical institutions. In the logic of constructivism, it is especially important that this fixes the electronic form as equivalent to the material one.

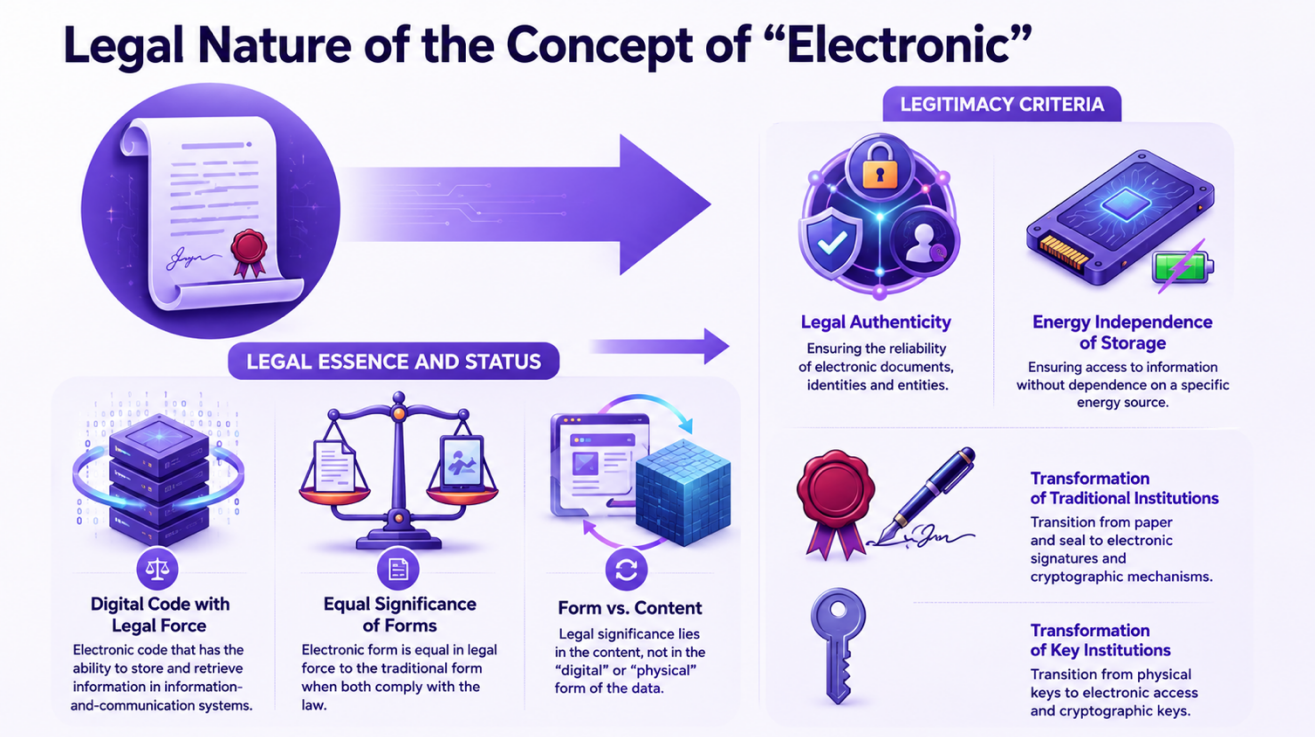


Figure 62. Definition of "electronic" from the standpoint of information law.

The definition *of "electronic"* from the standpoint of information law and digital law, first of all, emphasises its doctrinal correctness within the evolution of legal regulation of information processes and, at the same time, its clear place in the new paradigm of digital legal reality. It separates "electronic" as a form of legal implementation from "digital" as an ontological category of structured data and algorithmic processes, which is fundamentally important for the theoretical purity of the subject of regulation information as an object of creation, transmission, storage and use in information and communication systems (Figure 62).

Within the framework of information law, the emphasis on the requirements of authenticity, integrity, identification of subjects and preservation of information is especially significant. It is these criteria that form the core of information and legal regimes for information protection, electronic document management, electronic evidence and cybersecurity. From the standpoint of information law, this definition also demonstrates the transition from the perception of electronic as an auxiliary technological shell to its recognition as a full-fledged legal form of exercising rights and obligations. This is in line with modern trends in the development of e-governance, digital justice, digital services and digital administration, where electronic form is the basic way of legal interaction between the state, business and citizens.

In the Ukrainian legal field, there is no definition of "electronic" as a separate element or legal norm. The introduction of such a specific definition will create favourable conditions for modern recodification.

5.2. Digital jurisdiction as a post-territorial legal construction: theoretical and legal justification

5.2.1. Modern paradigms of legal regulation.

In the modern world, when the Metaverse is becoming an integral part of the digital landscape, the issue of its legal regulation becomes important. The cross-border nature of virtual ecosystems creates gaps in international law and national jurisdictions, which makes it impossible to ensure the territorialisation of the Metaverse, as well as the inability of states to ensure their sovereignty in the Metaverse, even by creating national Metaverses (Tsagourias, 2018)[1].

Modern paradigms of legal regulation are focused on the development of new hypotheses and models that take into account the specifics of the digital environment (Kostenko & Golovko, 2023b)[2]. These paradigms encompass both national and international approaches to regulating the rights and obligations of Metaverse participants, as well as issues of jurisdiction and enforcement of digital rights. The idea of the Metaverse digital jurisdiction paradigm is presented in order to create and provide a new legal framework for the functioning of digital societies in virtual environments (Kostenko et al., 2023a)[3].

A modern approach to Metaverse legal regulation is proposed, with a focus on the development of digital jurisdictions and the integration of legal regulations into digital spaces. This highlights the need for harmonisation of legal standards between different countries to ensure law and order in global digital ecosystems and effective interaction between users from different jurisdictions (Kostenko et al., 2022e)[4].

The Digital Jurisdiction Model is an innovative approach to legal frameworks designed to navigate complex digital interactions in the Metaverse and represents an innovative look at the evolution of legal regulation. Digital jurisdiction aims to create an effective system of legal regulation of virtual ecosystems and address important legal issues arising from the convergence of digital realities, including the creation of an electronic court system designed to ensure fair resolution of disputes regardless of geographical boundaries. Because virtual activities often cross state and national borders, it's important to understand the implications of personal jurisdiction in the context of digital transactions. Metaverse participants can inadvertently obey the legal standards of several jurisdictions, making it difficult to fulfil contracts and legal obligations (AlLouzi & Alomari, 2023)[5].

---

1 Tsagourias, N. (2018, July 13). *Law, borders and the territorialisation of cyberspace*. SSRN. https://doi.org/10.2139/ssrn.3213511

2 Kostenko, O., & Golovko, O. (2023). Metaverse electronic jurisdiction: Challenges and risks legal regulation of virtual reality. *Information and Law, 1(44),* 102–105. https://doi.org/10.37750/2616-6798.2023.1(44).278783

3 Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023a). Metaverse: Model criminal code. *Baltic Journal of Economic Studies, 9*(4), 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-14

4 Kostenko, O., Jaynes, T., Zhuravlov, D., Dniprov, O., & Usenko, Y. (2022e). Problems of using autonomous military AI against the background of Russia's military aggression against Ukraine. *Baltic Journal of Legal and Social Sciences, 4*, 131–145. https://doi.org/10.30525/2592-8813-2022-4-1

5AlLouzi, A., & Alomari, K. (2023). Adequate legal rules in settling metaverse disputes: Hybrid legal framework for metaverse dispute resolution (HLFMDR). *International Journal of Data and Network Science*, 7(4), 1665–1676. https://doi.org/10.5267/j.ijdns.2023.8.001.

The implementation of such a model faces difficulties related to the need for coordinated cross-border regulation, which is slow to adapt to the speed of technological progress.

Discussions in the academic community highlight the importance of anticipating and defining legal powers in these new spaces, as traditional legal frameworks may not adequately respond to the new interactions and transactions taking place in the Metaverse (Giancaspro, 2017)[1]. Today, apologists of analog law create significant obstacles to resolving issues related to the legal recognition of digital objects as objects endowed with the rights of an individual or legal entity or an authorised representative of a corporation in virtual ecosystems (Lee, 2022; Kostenko, 2022b)[2,3].

5.2.2 Code as the Constitution of Cyberspace: From Lessig to the Architecture of Digital Jurisdiction.

Cross-border digital spaces are shaping a new type of legal reality in which traditional instruments of analog law do not work properly. That is why there is a need for a new legal structure — digital jurisdiction, which is designed to respond to the challenges of the digital age. Currently, this approach has no analogues. The foundation of digital jurisdiction is the "Declaration of the Independence of Cyberspace" by J. P. Barlow, as well as "Code and Other Laws of Cyberspace" and "Code" by L. Lessig. It is the code that determines the ways, boundaries and order of interaction of users in cyberspace, just as in the physical world social relations are regulated by the norms of public administration and law. L. Lessig substantiates the thesis that in the fundamental dimension the code is a kind of "Constitution" of cyberspace, since it establishes the rules of access to digital environments, determines the boundaries of privacy, security, freedom of action of users and forms algorithmic control regimes. Thus, the code appears as a form of digital sovereignty that creates an autonomous order alternative to traditional models of legal and state regulation in the physical world.

The difference between the modern cyberspace Web 2.0 and Metaverse\Web 4.0 lies in the change in the very nature of legal relations. In the Web 2.0 system, the vast majority of processes are regulated by current regulations that cover a certain range of social relations. Instead, new types of digital interaction are emerging in the Metaverse that have no clear analogues in traditional law. They are aimed at determining their content, focus and legal status — that is, at creating a basis for the formation of adequate mechanisms for their regulation. The key questions remain: what meaning should be put into the concepts *of "social relations in the Metaverse"* and *"relations in the Metaverse"*; under what conditions electronic subjects and objects can be endowed with human rights; what forms of justice can be applied in the virtual environment; what responsibility will electronic subjects and objects endowed with human rights have.

---

1 Giancaspro, M. (2017). Is a “smart contract” really a smart idea? Insights from a legal perspective. *Computer Law & Security Review, 33*(6), 825–835. https://doi.org/10.1016/j.clsr.2017.05.007

2 Lee, J. (2022). A legal brief study of metaverse. *Liberal Arts Innovation Center*, *10*, 63–74. https://doi.org/10.54698/kl.2022.10.63

3 Kostenko, O. V. (2022). Electronic jurisdiction, metaverse, artificial intelligence, digital personality, digital avatar, neural networks: Theory, practice, perspective. *World Science, 73(1),* 1–13. https://doi.org/10.31435/rsglobal_ws/30012022/7751

We propose the following author's definition of "social relations in the Metaverse" — *this is a set of socially significant, normatively relevant interactions between subjects that arise, are carried out and transformed in immersive digital environments of the Metaverse using information and communication, algorithmic, immersion and distributed technologies, and have the potential or ability to be regulated by the norms of law, in particular information and digital law, regardless of their direct formalisation at the time of occurrence.*

From the standpoint of the general theory of law, social relations are traditionally considered as an objective social reality that precedes legal regulation and constitutes its subject. In this sense, social relations in the Metaverse are no exception, but they are characterised by fundamentally new features associated with the digital form of their existence, immersion, algorithmic mediation and transnational character. In contrast to classical social relations that are formed in the physical social space, social relations in the Metaverse arise in an artificially constructed digital environment, where social interaction is mediated by code, protocols, interfaces, and artificial intelligence systems. They encompass economic activity, communication, cultural interaction, education, labour, self-government, identification, and social stratification, however, they are realised through digital identities, avatars, digital twins, and other derived forms of presence. From the point of view of information law, the key feature of such relations is that their content and material basis are information and data: personal, behavioural, transactional, spatial, biometric, etc. At the same time, it is important to emphasise that not all social relations in the Metaverse immediately acquire the status of legal relations. Some of them are at the pre-conventional or pre-legal level, but already contain the potential for normative ordering. That is why the category of "social relations in the Metaverse" is broader than "relations in the Metaverse" in a narrow, legal sense and performs a methodological function to determine the subject of future legal regulation.

We propose the following author's definition of "relations in the Metaverse" — *these are legally significant, normatively defined or subject to normative recognition, interactions between subjects in immersive digital environments of the Metaverse, which arise in relation to information, data, virtual assets, digital identity, algorithmic solutions and other digital objects and are implemented using information, algorithmic, immersion and distributed technologies within the relevant legal regimes.*

Unlike social relations, relations in the Metaverse in this sense have a clearly expressed legal character. They are either already regulated norms of law, or those that are recognised by law as legally significant and capable of generating legal consequences. Thus, we are talking about a specific type of legal relations that are implemented in a digital, immersive environment. These relations retain the classical structural model of legal relations (subjects, objects, content), but are filled with new content. The subjects are not only individuals and legal entities, but also digital entities of a derivative nature — avatars, digital twins, autonomous agents. Objects are not tangible things, but virtual assets, digital property, data, accesses, algorithmic decisions and the results of the functioning of digital systems. In the field of information law, the decisive circumstance is that most of the relationships in the Metaverse arise precisely about information — its collection, storage, processing, transfer, use, and protection. This applies to both personal

data of users and non-personalised data that form digital profiles, ratings, behavioural models, and the economic value of subjects in the Metaverse.

A feature of relationships in the Metaverse is also the algorithmic mediation of their occurrence and implementation. Legally significant actions can be carried out automatically — through smart contracts, protocol rules, or decisions of artificial intelligence systems. This necessitates a rethinking of such categories as expression of will, attribution of actions, responsibility and proof, which already goes beyond the boundaries of classical private or public law and requires

Thus, relations in the Metaverse should be considered as a new form of legal relations integrated into the digital architecture of the environment, in which law functions not only as an external regulator, but as an internal element of digital processes. It is these relations that constitute the direct subject of digital jurisdiction and form the core of the legal order in the Metaverse.

The modern Metaverse is evolving from imitating the real world to developing on its own, forming a new system of values, legal norms, and even social hierarchies that are gradually beginning to affect the real world.

The main problem remains the lack of a single legal mechanism for regulating social relations in the Metaverse. Most national legal systems are based on regulations created without taking into account the technological nature of the Metaverse. At best, the current legislation only partially covers certain aspects of digital interaction, leaving significant areas in a state of legal uncertainty.

Attempts to modernise the legal system often boil down to the adoption of temporary bylaws or departmental instructions that do not provide a systematic approach. Judicial practice is just beginning to form precedents for e-justice, applying the current norms of analog law to digital cases. This forms the basis for the future of digital justice, but today such solutions are fragmented.

The diversity of legal cultures and state interests creates an asymmetry of regulation: what is considered an offence in one country can be considered as a lawful action in another. As a result, even progressive regulations are often declarative in nature and do not provide real legal action. Despite this, Metaverse technologies are already giving rise to new types of legal relations that require regulation. That is why the task of creating a systemic legal framework of the Metaverse arises, which will ensure the coherent coexistence of human, technology and algorithm within a single digital legal order (Kaddoura & Husseiny, 2023)[1].

Total digitalisation demonstrates the crisis failure of analog law in digital ecosystems — analog law historically relies on three "pillars": territoriality (lex loci), materiality of objects (res), and centralised institutions of coercion. Materiality is inferior to digital things or quasi-things — states of program code (tokens, on-chain records, accesses, nodes), for which classical real estate structures do not work without special modifications. Coercion is increasingly implemented by self-execution protocols (smart contracts, oracles, access lists) that operate outside the traditional court-executor vertical.

1 Kaddoura, S., & Husseiny, F. (2023). The rising trend of metaverse in education: Challenges, opportunities, and ethical considerations. *PeerJ Computer Science, 9*, e1252. https://doi.org/10.7717/peerj-cs.1252

A regulatory lag arises: the rule-making cycle of states is years; while the digital protocol cycle is weeks (Dwivedi et al., 2022)[1].

Classic conflict-of-laws bindings (place of conclusion/performance, nationality of the parties, location of the thing) lose relevance if the parties are network identities (DID/VC) and the "thing" is the state of the distributed ledger. Procedural proofs also remain insufficient: the admissibility of cryptographic signatures, transaction logs, timestamps, and chain of custody requires a stand-alone procedural framework that describes cryptographic verification, replication, and finality of records.

The cross-border nature of electronic ecosystems (e-ecosystems) and the Metaverse forms new principles for the functioning of society (Mascitti, 2024)[2].

E-ecosystems and the Metaverse are inherently cross-border and international, as they are organised according to protocol principles, and not along state borders. Their basic principles of functioning are defined as follows:

1) jurisdiction of data and protocols instead of exclusively territorial jurisdiction;

2) protocol governance (on-chain voting, multi-signature, delegation) along with public law verticals;

3) self-fulfilment and "soft coercion" through changes in access rights, freezing of assets, etc.;

4) identity as a set of attributes that requires the legal status of avatars, AI agents, and DAOs;

5) objects as code states (on-chain assets, tokenised rights, access licences);

6) event-driven, which requires legal orchestrations mapped to event bus protocols.

Accordingly, the law should function at the level of protocols and data, which justifies the emergence of digital jurisdiction as a special regulatory shell with new "legal anchors": provenance anchors (origin and quality of data), infrastructure (node location, HSM/TEE), identification (DID/VC), economic (on-chain activity nexus), as well as lex protocolli as a special form of lex specialis for smart contracts and consensus mechanisms.

5.2.3. The End of the Peace of Westphalia: Law in the Age of Protocols and Platforms.

The Westphalian paradigm was based on the principles of territorial integrity and the state's monopoly on law and coercion (Johnson & Post, 1996).[3] In the digital age, it is degrading due to: blurring of boundaries by data flows; the emergence of parallel legal orders (platforms, protocols, private standards); asymmetry of capacities between states and transnational technological networks. As a reaction, a phenomenon is formed that can be described as "Balkan cyber sovereignty". This is a mosaic fragmentation of the

---

1 Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., Janssen, M., Kim, Y. G., Kim, J., Koos, S., Kreps, D., Kshetri, N., Kumar, V., Ooi, K. B., Papagiannidis, S., Pappas, I. O., Polyviou, A., Park, S., Pandey, N., Queiroz, M. M., Raman, R., Rauschnabel, P. A., Shirish, A., Sigala, M., Spanaki, K., Tan, G. W. H., Tiwari, M. K., Viglia, G., & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

2 Mascitti, M. (2024). The metaverse impact on the politics means. *Computer Law & Security Review, 55*, 106037. https://doi.org/10.1016/j.clsr.2024.106037.

3 Johnson, D. R., & Post, D. G. (1996). Law and borders—The rise of law in cyberspace. *Stanford Law Review, 48*(5), 1367–1402. https://doi.org/10.2139/ssrn.535

network space (cyber sovereignty) on the basis of data localisation, national crypto lagoons, licensing of data centres, barriers to cross-border information transfer, and "digital borders" for AI and crypto infrastructures.

Signs of this state: regulatory "iron tent" (data localisation, sovereign clouds); jurisdictional maneuvering (selection of favourable regimes for protocols); Splinternet (incompatible technical and legal standards) proxy sovereignty of platforms (community rules and terms of service that actually perform quasi-state functions); sanctions regimes as tools of cyber geopolitics.

The consequence is the blocking of interoperability and the growth of transaction costs for innovation. Therefore, a digital jurisdiction should introduce "bridges of trust": mutual recognition of DID/VC, inter-jurisdictional rules for the admissibility of digital evidence, interoperability standards for smart contracts, and cloud AI-judiciary as supranational dispute resolution mechanisms.

Thus, digital jurisdiction is a new phenomenon of the digital space environment. In a conceptual sense, digital jurisdiction is a cardinal difference from electronic legal relations. If *electronic legal relations* determine the technological basis — electronic documents, transactions, infrastructure — then *digital jurisdiction* covers the full lifecycle of data, algorithms, rights, and ethical norms, including autonomous artificial systems, decentralised organisations (DAOs), and virtual identities. Thus, digital includes electronic as a technical layer, but expands it to the algorithmic, legal, semantic, and ethical-social dimensions, forming a new architecture of legal sovereignty — *Meta-Legal OS*.

Unlike classical territorial forms of justice, digital jurisdiction is based on the principle of functional presence: the legal consequences of actions are determined not by geography, but by the digital field (location) where the activity took place or data that gives rise to legal consequences is stored. This approach ensures extraterritoriality, flexibility and the ability of the state to protect the rights of its citizens in global cyberspace, where borders are determined not by borders, but by data, network connections and digital identities.

The state ensures the legitimacy, publicity and transparency of digital jurisdiction; creates institutions that implement justice in digital format; guarantees the identification and verification of each entity in the virtual environment, as well as preserves its legal personality in the event of cross-border interaction.

Such institutions include digital courts, digital arbitrations, online notaries, registers of electronic decisions, automated evidence verification systems, and legal monitoring services. They operate on the basis of smart contracts, blockchain records, and transparent decision-making algorithms involving human-controlled artificial intelligence.

Digital jurisdiction operates on the principles of digital sovereignty, the rule of law, respect for human rights, algorithmic justice, compatibility of legal systems, ethical responsibility and international cooperation. It provides for the mandatory provision of open access to legal acts, appeal procedures in electronic format and mechanisms for cross-border enforcement of decisions through international digital law platforms. Digital jurisdiction applies to:

legal relationships arising within digital platforms, blockchain networks, Metaverse, decentralised autonomous organisations (DAOs), virtual offices, government portals, smart ecosystems, digital exchanges, educational and communication environments,

including immersive platforms that enable interaction between humans and artificial agents;

electronic transactions, administrative procedures, judicial proceedings, certification, licensing, registration, electronic notarisation, digital transactions and other legally significant actions carried out in a virtual environment and generating legal consequences in a digital or mixed format;

electronic evidence, digital identity, smart contracts, decentralised agreements, blockchain records, electronic archives, digital certificates, biometric confirmations, and other forms of interaction that have legal significance and ensure the authenticity, reliability, and reproducibility of legal facts in the digital environment.

5.3. Digital Jurisdiction Model in the Metaverse Environment: Structural and Functional Analysis

Digital jurisdiction is a multidimensional legal form of exercising jurisdictional powers in the digital environment, which ensures the full functioning of the legal system in the Metaverse virtual space and e-ecosystems. So, let's consider the author's definition of "digital jurisdiction".

"*Digital jurisdiction is a post-territorial or cross-border legal construct that regulates social, economic, informational, and algorithmic relations in digital ecosystems — cyberspace, blockchain networks, artificial intelligence environments, and the Metaverse. It encompasses a set of technical, procedural, regulatory and ethical principles that determine the order of access, interaction, identification, digital social relations, digital rights, digital obligations, digital responsibility, as well as the functioning of the digital judicial system in the digital environment*", or compactly, then

"Digital jurisdiction" is a systematically organised legal regime for the regulation, recognition and provision of legally significant actions, decisions and legal relations that arise, are carried out and recorded in the digital environment, regardless of the territorial location of subjects, with or without human participation, with the use of information, algorithmic, immersion and distributed technologies".

Digital jurisdiction encompasses a set of norms, principles and mechanisms that determine: the legal status of digital actors, including digital identities, avatars, digital twins and autonomous agents; conditions for the occurrence, implementation and termination of rights and obligations in the digital environment; rules for the circulation and protection of virtual assets, digital property and data; admissibility, authenticity and legal force of digital evidence; mechanisms of responsibility for violations committed in the digital environment.

Digital jurisdiction is not limited to the procedural form of exercising power or judicial powers, but extends to the very architecture of the digital environment, within which code, algorithm, protocol and artificial intelligence can perform quasi-normative and regulatory functions.

In digital jurisdiction, the "place" of legal relations is recognised not as the territory of the state, but as a digital space or cluster (location) of digital infrastructure, which forms a post-territorial model of the legal order. It is in this model that the coexistence and interaction of multiple jurisdictions — state, platform, decentralised and hybrid — is possible. Digital jurisdiction is a logical stage in the evolution of jurisdiction and forms

the core of a new paradigm of digital law, in which law is integrated directly into the digital architecture of social relations.

The proposed definition of digital jurisdiction fixes a fundamentally new approach to understanding jurisdiction in the digital environment, which goes beyond the classical territorial-state vision of jurisdiction and relies on the post-territorial logic of the digital legal order. Unlike traditional doctrines linking jurisdiction with the territorial sovereignty of the state, the hierarchy of public authorities and the monopoly on the exercise of powers, digital jurisdiction appears as a systematically organised legal regime integrated directly into the architecture of digital space, digital platforms, immersion environments and distributed infrastructures.

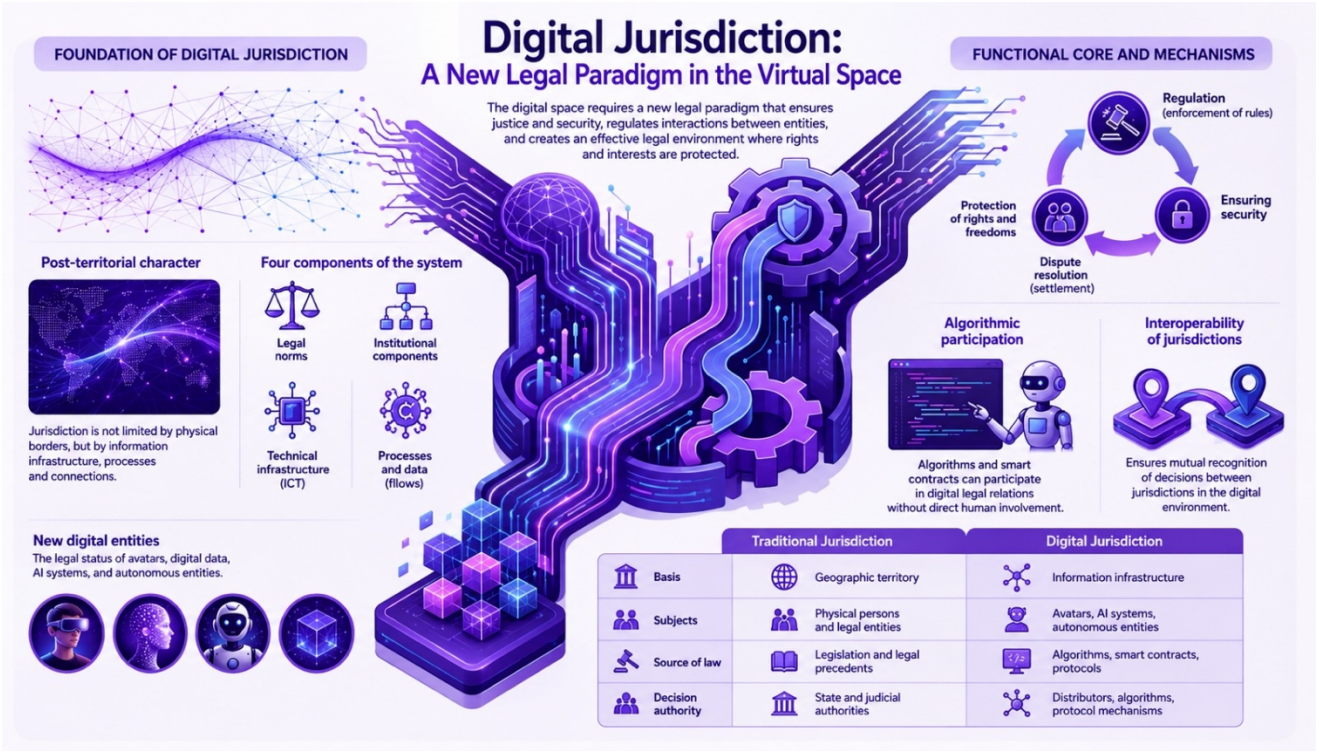


Figure 63. Digital jurisdiction.

In this approach, jurisdiction ceases to be considered exclusively as an external instrument of law enforcement and is transformed into an internal property of the digital environment, within which the legal significance of actions, decisions and legal relations is determined not only by the norms of positive law, but also by technical and algorithmic mechanisms for their implementation. That is why digital jurisdiction is conceptualised as an ontological element of digital law, which forms its own legal space, in which law, technology and infrastructure are in a relationship of mutual conditionality (Figure 63).

This approach allows us to move from an instrumental understanding of jurisdiction, which is characteristic of e-governance and e-justice, to its ontological understanding within the framework of digital law, where jurisdiction becomes a characteristic of the digital environment itself, and not only the activities of state or quasi-state institutions.

The key is that digital jurisdiction is not reduced to a set of procedural rules, technical procedures or electronic services designed to serve traditional jurisdictional mechanisms. Unlike electronic legal relations, which mainly provide a digital form of

implementation of existing law enforcement procedures, digital jurisdiction covers the full cycle of legal significance in the digital environment as a holistic and continuous process.

Such a cycle includes the stage of emergence of a digital legal fact (transaction, algorithmic decision, protocol event, avatar or autonomous agent action), its initial technical and legal fixation in the form of a digital trace or entry in an information system or distributed ledger, further regulatory recognition of this fact as legally relevant, as well as the possibility of its use in evidentiary activities and law enforcement.

The final element of this cycle is enforcement of legal consequences, which in a digital jurisdiction can combine traditional legal enforcement mechanisms with technical and algorithmic enforcement tools, including smart contracts, protocol restrictions, and automated controls. It is this continuity and internal coherence of the stages of legal significance that distinguishes digital jurisdiction from its electronic predecessors and confirms its systemic nature.

The systematically organised legal regime, internal architecture and use of the category of "legal regime" emphasise the complex, multi-level nature of digital jurisdiction as a special form of legal ordering of digital social relations. It is not about a mechanical combination of individual legal norms or procedures, but about an integral regulatory structure, within which substantive, procedural, institutional and technological elements function in interconnection and mutual conditioning.

The substantive component of digital jurisdiction determines the legal status of digital entities, the regime of digital objects, virtual assets and data, as well as the content of rights and obligations arising in the digital environment. The procedural component covers the rules for fixing legally significant actions, algorithmic decisions and digital events, the procedure for their recognition, proof, appeal and enforcement of legal consequences. The institutional component includes both classical government agencies and new digital institutions — platform operators, decentralised autonomous organisations, digital identity providers, and infrastructure actors.

The technological component of digital jurisdiction forms its integral basis and includes information systems, algorithmic models, immersion environments, distributed registers and protocols within which legal relations are implemented. In the digital environment, these elements cannot exist in isolation, since the legal significance of actions and objects directly depends on the architecture of the digital infrastructure, its technical parameters, access rules and control mechanisms. That is why digital jurisdiction provides for the integration of legal regulation into the technological environment as a necessary condition for the effectiveness and effectiveness of the digital legal order.

Digital jurisdiction forms its own legal ontology, within which data, algorithms, program code, smart contracts, and interaction protocols are recognised not only as technical elements of digital infrastructure, but also as carriers of regulatory relevance. In such an ontology, legal significance arises not exclusively from the text of the normative legal act, but from the combination of legal prescriptions with algorithmic rules, protocol restrictions, and architectural solutions of the digital environment.

This means that law in a digital jurisdiction ceases to be an exclusively external regulator of behaviour and acquires the features of an internal structural element of a

digital system. The rules of law can be implemented in the form of machine-readable rules, access parameters, conditions for the execution of smart contracts or decision-making algorithms, which ensures their direct action in the digital environment.

In view of the above, digital jurisdiction necessitates the integration of legal regulation directly into the digital architecture, and not only its external application through traditional law enforcement mechanisms. It is this integration that creates the basis for the formation of a stable and predictable digital legal order, in which regulatory prescriptions, algorithmic processes and infrastructure solutions form a single regulatory system.

The definition of "digital jurisdiction" contains three interrelated and interdependent functions — regulation, recognition and enforcement, which together form the functional core of the digital legal order.

Regulation within digital jurisdiction consists not only in establishing general rules of conduct, but also in the normative definition of the legal status of digital entities, modes of functioning of digital identities, avatars, digital twins and autonomous agents, as well as in establishing special rules for the creation, circulation, use and termination of digital objects, virtual assets and data. Unlike classical legal regulation, digital regulation relies heavily on a combination of regulations with algorithmic and protocol rules that operate directly in the digital environment.

The recognition function ensures the transformation of digital events and actions into legally significant facts. The recognition encompasses the giving of legal validity to digital transactions, acts of digital identification, the results of smart contract execution, the decisions of decentralised management systems, and the algorithmic decisions of artificial intelligence systems. This function is of particular importance in the cross-border digital environment, where the legal significance of digital events depends on the mechanisms of mutual recognition between different digital and electronic jurisdictions.

Enforcement in a digital jurisdiction combines classic legal mechanisms of liability, enforcement, and enforcement of rights with technical guarantees of data integrity, authenticity, immutability, and traceability. It is about the use of cryptographic methods, distributed ledgers, event logs and algorithmic control mechanisms that ensure the actual implementation of legal prescriptions and decisions in the digital environment. It is the integration of legal and technical means of support that distinguishes digital jurisdiction from traditional models of law enforcement.

It is the combination of these three functions that allows a digital jurisdiction to play the role of a full-fledged legal order in the digital environment, and not just an auxiliary procedural tool.

Digital jurisdiction covers not only judicial or administrative decisions in their classical sense, but the whole range of legally significant actions, events, decisions and legal relations that arise and are implemented in the digital environment. We are talking about such actions and events that cause the occurrence, change or termination of rights and obligations directly as a result of the functioning of digital systems, and not only as a result of the formalised expression of the will of public authorities: transactions with virtual assets and digital property carried out in distributed ledgers; actions of avatars and digital twins in immersive Metaverse environments, which may have property, non-property, or tort consequences; algorithmic decisions of artificial intelligence systems, in

particular in the field of content moderation, access to resources, automated compliance, or risk management; as well as protocol decisions of decentralised networks and decentralised autonomous organisations (DAOs), which are adopted by consensus and directly affect the legal status of participants.

In this context, digital jurisdiction captures a fundamental transformation of the very nature of a legally significant decision: it can be not only institutional-power, but also algorithmic or protocol in nature. That is why jurisdiction in digital law ceases to be exclusively an attribute of state power and acquires a multi-level, networked and functionally distributed character, which corresponds to the architecture of modern digital and immersion environments. Thus, jurisdiction in digital law ceases to be an exclusive attribute of state power in the classical public law sense and is transformed into a multi-level, networked and functionally distributed property of the digital legal order. It is implemented simultaneously at the level of state legal systems, platform regulatory regimes, decentralised protocol structures and hybrid management models that coexist and interact within a single digital environment.

Under such conditions, jurisdiction is determined not only by the subject of power, but also by the architecture of the digital infrastructure, the rules for the functioning of platforms and protocols, as well as algorithmic mechanisms for decision-making and implementation. This leads to a transition from a hierarchical model of jurisdiction to a network one, in which the law performs a coordination and integrative function between multiple centres of normative influence.

In digital law, the territory of the state ceases to be the only point of localisation of legal relations, since the legal relations themselves arise, develop and terminate in an environment that is by its nature cross-border, network and technically distributed. Instead, it attaches to a digital space or a specific cluster of digital infrastructure, which includes platforms, protocols, distributed ledgers, network nodes, Metaverse immersion environments, and other elements of digital architecture. It is the belonging of legal relations to a certain infrastructure ecosystem that determines the applicable rules, recognition mechanisms, evidentiary procedure, and liability models.

This approach means a transition from the territorial model of jurisdiction to the infrastructural-functional model, within which legal competence is formed depending on the architecture of the digital environment, its protocol rules, management models and technical parameters. This allows for a conceptual justification of the post-territorial nature of digital jurisdiction and creates a basis for the regulation of legal relations in global digital ecosystems, including the Metaverse, decentralised networks, and hybrid platform environments.

This approach makes it possible to theoretically and normatively explain the coexistence and interaction of multiple jurisdictions — state, platform, decentralised and hybrid — within a single digital space, without reducing them to a hierarchical model of subordination. Instead, jurisdictions are considered as functionally interacting regulatory regimes, each of which implements its own scope of regulatory influence in accordance with the architecture of the digital environment and the nature of legal relations.

It is in this logic that the basis for the development of legal interoperability mechanisms aimed at mutual recognition of digital identities, legal statuses, transactions, algorithmic decisions and digital evidence between different jurisdictional regimes is

formed. Legal interoperability in digital jurisdiction appears not as a purely technical compatibility of systems, but as a complex legal mechanism for harmonising norms, procedures and protocol rules, which ensures the integrity and continuity of the digital legal order in global and cross-border digital ecosystems.

A feature of digital jurisdiction is the ability to perform legally significant actions both with and without the direct participation of a person, in a fully or partially automated mode. In the digital environment, smart contracts, autonomous software agents, algorithmic modules, and artificial intelligence systems are able to independently initiate, execute, and complete actions that directly generate legal consequences in the form of the occurrence, modification, or termination of rights and obligations.

Unlike the classical legal model, in which a legally significant action is inextricably linked with the human expression of will, digital jurisdiction fixes the possibility of delegated or indirect expression of will, implemented through predetermined algorithmic rules, program code or protocol conditions. In such a model, the primary will of a person can be expressed at the stage of creating, configuring or activating an algorithmic system, while further actions occur autonomously, without constant human control.

This necessitates a doctrinal rethinking of the categories of expression of will, attribution of actions and legal responsibility in law. Attribution of legal consequences in a digital jurisdiction requires taking into account the complex chain of interaction between the algorithm developer, the operator of the digital system, the user who initiated its application, and the autonomous system itself. Liability in such cases cannot be based solely on traditional models of guilt or direct intent, but must take into account the degree of autonomy of the algorithm, the level of predictability of its behaviour, and the availability of control and intervention mechanisms.

In view of the above, digital jurisdiction forms the basis for the development of special regimes of algorithmic responsibility, delegated legal capacity, and procedures for appealing automated decisions. It is within the digital jurisdiction that it becomes possible to regulate the relationship between human and algorithmic participation in legal relations, which is of key importance for the legal support of the functioning of artificial intelligence, autonomous agents and immersive digital environments.

Digital jurisdiction should lay down clearly defined and normatively enshrined rules for delegating, controlling and appealing algorithmic decisions operating in the digital environment. Such rules should define the conditions for the admissibility of delegating legally significant actions to algorithmic systems, the limits of the autonomy of their functioning, standards of human supervision, as well as procedures for intervention in case of errors, failures or violations of the rights and legitimate interests of subjects.

Striking a balance between automation and legal safeguards in a digital jurisdiction means combining the efficiency of algorithmic processes with the principles of legal certainty, accountability, transparency, and access to remedies. It is through the regulatory regulation of delegation, control, and appeal of algorithmic decisions that digital jurisdiction ensures the legitimacy of the use of artificial intelligence and autonomous systems and prevents the transformation of the digital environment into an uncontrolled space of technical regulation, separated from the legal order.

The place of digital jurisdiction in the structure of law. Based on the analysis, it is advisable to consider digital jurisdiction as the core of a new paradigm of digital law,

which performs a system-forming function in the formation of the digital legal order. It is within the framework of digital jurisdiction that there is a conceptual combination of material, procedural and technological aspects of legal regulation, which exist relatively autonomously in traditional branches of law.

The material dimension of digital jurisdiction determines the legal status of digital subjects, objects and assets, forms the content of rights and obligations in the digital environment and lays the foundations for new legal regimes, in particular with regard to virtual assets, digital identity and data. The procedural dimension provides normative certainty for the processes of occurrence, recognition, proof, appeal and implementation of legally significant actions and decisions in the digital environment. The technological dimension, in turn, integrates legal regulation directly into the digital architecture of social relations through algorithms, protocols, smart contracts and immersion environments.

Thus, digital jurisdiction does not provide external imposition of legal norms on digital processes, but their internal incorporation into the architecture of the digital environment. This allows us to consider it as a conceptual basis of digital law, within which the law functions not only as a system of prescriptions, but as an integrated regulatory element of digital ecosystems, ensuring the integrated regulation of the Metaverse, artificial intelligence, and immersion technologies within a single legal order.

5.4. Mechanisms for the implementation of digital jurisdiction in the context of the development of the Metaverse

5.4.1.Mechanisms for the legal regulation of social relations in the Metaverse

The creation of mechanisms for the legal regulation of social relations in the Metaverse should solve many legislative problems related to differences in the regulations of different jurisdictions. Most legal systems have existing archaic regulations, which are formulated without taking into account the possible emergence of social relations using Metaverse electronic technologies (Nguyen et al., 2023)[1]. In some cases, these laws may regulate certain issues of the use of information technologies, but the scope of their application is often either narrow or ambiguous, which creates a situation of certain legal uncertainty.

Digital jurisdiction and digital justice are one of the key elements of electronic social relations in the Metaverse. Digital justice at the initial stage can be based on traditional "analog" justice, which is transformed in accordance with the development of electronic social relations in the Metaverse. Blockchain and AI will play an important role in the functioning of digital jurisdiction (Figure 64), which will provide legal regulation of Metaverse subjects and objects – Personal Metaverse (PM), Collective Metaverse (CM), Corporate Metaverse (CorpM), Confederate Metaverse (CfM), State Metaverse (SM), and Megametaverse (Hayes & Boyle, n.d.)[2].

1Nguyen, C., Hoang, D., Nguyen, D., Xiao, Y., Niyato, D., & Dutkiewicz, E. (2023). MetaShard: A novel sharding blockchain platform for metaverse applications. *arXiv,* 1–12. https://doi.org/10.48550/arXiv.2305.00367

2 Hayes, A., & Boyle, M. J. (n.d.). What is the European Union (EU)? *Investopedia*. https://www.investopedia.com/terms/e/europeanunion.asp

Thanks to blockchain technology, it is possible to overcome the crisis of trust in the state and other institutions, because the use of the services of the state or intermediaries in the financial services market is, on the one hand, forced due to an authoritative order, but, on the other hand, attractive due to certain guarantees that they provide to the user



Figure 64. Interaction of subjects and objects in digital jurisdiction

The formation of legal norms regulating the use of distributed ledger technologies (blockchain) within the framework of information law is an objective response to the transformation of modes of creating, storing, processing and verifying information in the digital environment. In this context, it is advisable to consider blockchain not as an independent financial or organisational innovation, but as an information technology infrastructure that provides a specific regime for fixing data, its integrity, authenticity and traceability, which directly affects the emergence of legally significant facts.

Information circulating in digital networks and immersion environments of the Metaverse (European Commission, n.d.; Kodem et al., 2023)[1, 2],acquires the status of a key resource of legal regulation, since it forms the basis for the formation of rights, obligations and legal consequences. Within the framework of information law, such information is considered not only as an object of protection or access, but as an element of the legal infrastructure in which data performs the function of a carrier of legal significance. Accordingly, the transformation of social relations in the digital environment leads to a change in traditional models of information flow management and a gradual decrease in the effectiveness of hierarchical, centralised control mechanisms.

The use of distributed ledger technologies leads to a redistribution of information control functions, in particular in the field of financial data, transactional information, and the circulation of digital assets (Yang et al., 2022; Tabatabaei et al., 2023; S S. N. et al., 2023). From the standpoint of information law, this means that the state loses its monopoly position as the only guarantor of the reliability and legitimacy of information records, while technically determined verification mechanisms that operate on the basis of cryptographic and protocol rules appear. Such mechanisms do not replace legal regulation, but significantly change its tools and subject.

In this context, decentralised autonomous organisations (DAOs) appear as a special information and legal construct, within which management is carried out not through the organisational and administrative apparatus, but through the processing and execution of algorithmically determined rules (Kostenko et al., 2022f).[3] From the information and legal point of view, DAOs are systems for organising information processes, in which smart contracts perform the function of regulatory instructions, and entries in distributed ledgers perform the function of official information sources about legally significant actions and decisions.

The lack of a traditional structure of governing bodies and personified officials in DAOs complicates the application of classical models of legal responsibility, in particular in criminal and administrative law. However, from the standpoint of information law, the key is not to identify a specific individual, but to determine the regime of responsibility for the creation, modification and operation of information systems and algorithms, within which legally significant consequences are formed. It is the information and legal approach that allows us to shift the emphasis from personalised responsibility to responsibility for the management of information processes and digital infrastructure.

Based on the above, we can conclude that blockchain and DAOs do not require fragmentary regulation within individual industries, but systemic inclusion in the subject of information law as special modes of data circulation and algorithmic information processing. This approach creates a methodological basis for the further development of digital law and the formation of models of electronic and digital jurisdiction, in which information is recognised as a central element of the legal order.

---

1 European Commission. (n.d.). *Legal and regulatory framework for blockchain*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain

2 Kodem, S., Singh, H., Kumar, S. R., Patel, H. N., Chandan, R. R., & Karthikraj. (2023). Integration of blockchain technology in metaverse for future era of digital businesses. In *Proceedings of the 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)* (pp. 522–526). https://doi.org/10.1109/UPCON59197.2023.10434472

3 Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022f). Genesis of legal regulation web and the model of the electronic jurisdiction of the metaverse. *Bratislava Law Review, 6(2),* 21–36. https://doi.org/10.46282/blr.2022.6.2.316

The formation of law in the Metaverse objectively begins with the stage of projection of the laws of physical society on electronic social relations. But, given the fact that the Metaverse is comprehensive, the projection of the laws of different countries will not have the desired effect. This provides an impetus for the modernisation and improvement of national legislation in the field of optimisation and increasing the efficiency of its use.

The legal regulation of social relations in the Metaverse requires the development of a comprehensive digital jurisdiction based on the latest basic legislation — the Metaverse Magna Carta (GLM). In our opinion, the GLM should include the following key parts: the Constitution. Magna Carta; General Norms, Composition of Magna Carta Laws; WM Common Law; WM Judicial System; WM Electronic Office Law; WM Cross-Border Interaction Act; Code fundamental technical regulations of WM; WM Identity Management Certificate; WM Code of Non-Property Electronic Assets; WM Criminal Electronic Code; WM Cyber Protection Code; WM Military Regulations; Large electronic court code WM; Other regulatory legal acts.



Figure 65. Model of complex digital jurisdiction

Digital jurisdiction, digital justice is one of the key elements of digital social relations in the Metaverse. Digital justice at the initial stage can be based on traditional "analog" justice, which is transformed according to the development of digital social relations in the Metaverse (Figure 65).

The creation of mechanisms for the legal regulation of social relations in the Metaverse should solve many legislative problems related to differences in the regulations of different jurisdictions governing the use of information and communication technologies, identification procedures, copyright, ownership of non-property assets, liability for causing damage, the list of crimes and coercive measures of the state for their commission.

The current "legislation of the analog era" should be taken as a basis and begin to form a Magna Carta of Metaverse laws. The Constitution, the Statutes, the common law, the judicial system must have structures that contribute as much as possible to the democratic and legitimate functioning of the WM.

A set of fundamental technical regulations — technical and legal documents that should fix the reference program codes that will be used to determine at the legislative level the legal status and ownership of non-property electronic assets, such as NFTs or content.

The WM Code of Non-Property Digital Assets is designed to regulate relations with non-property assets and establish the right of electronic property and electronic intellectual property. The Criminal Digital Code WM is designed to determine the types of offences with the development and use of information and communication technologies and Metaverse technologies, as well as the establishment of state and other coercive measures in case of offences. The Cybersecurity Code — a technical and legal document that should establish at the legislative level reference programs, administrative, managerial and technical measures to ensure cybersecurity, which will be mandatory for all subjects and objects of WM. The WM Large Digital Judicial Code will contain rules and algorithms for digital jurisdiction, will determine its subjects, objects, territoriality, specialisation, etc. In fact, it is the core of WM's digital jurisdiction (Figure 66).

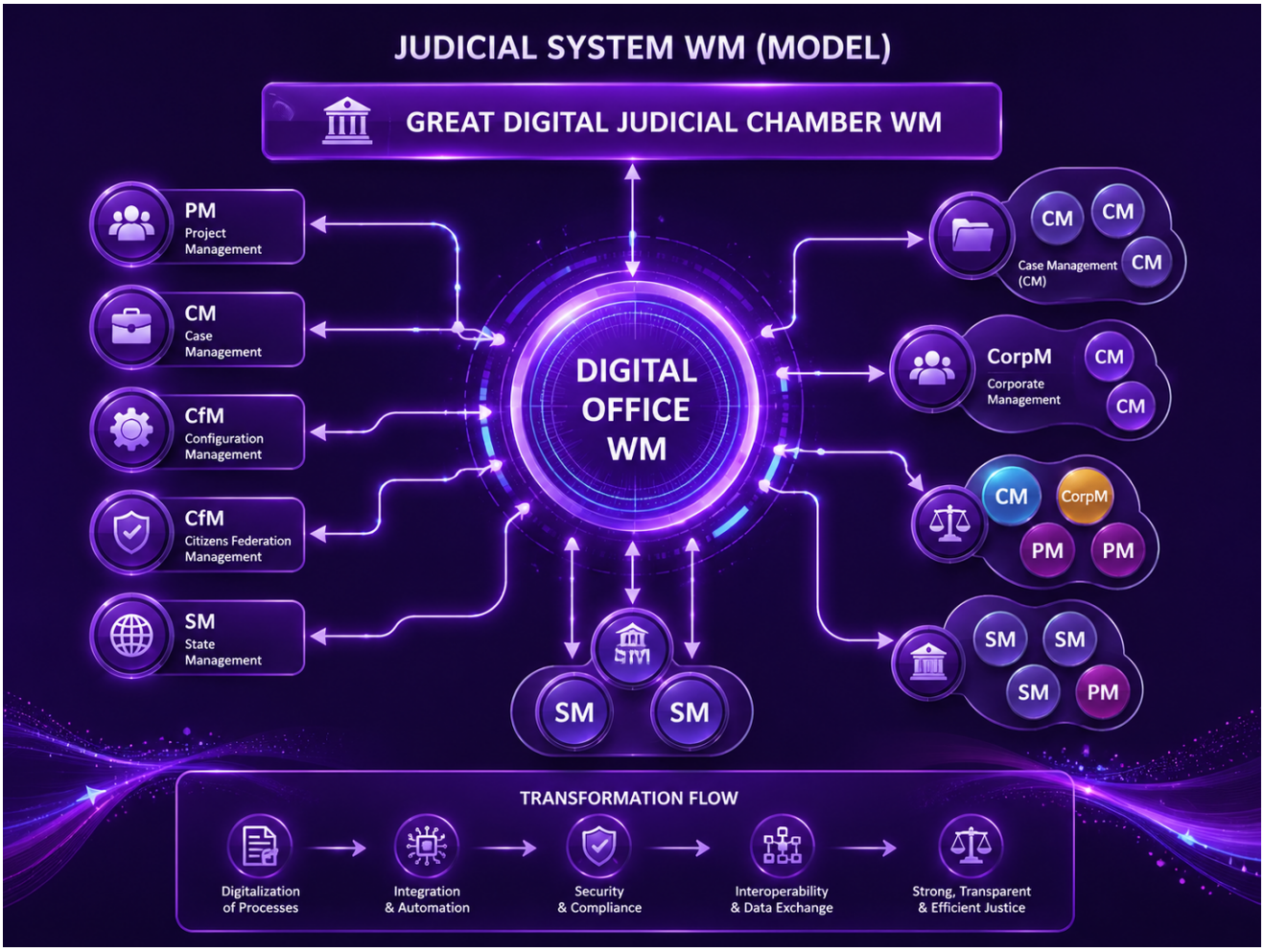


Figure 66. WM Digital Office

The WM Digital Office will work with the use of AAI and ASI and will perform the tasks of the Central Analytical Center and the Administrator of Electronic Reports on Electronic Incidents (Electronic Offenses). The WM Digital Office will accept requests for e-incidents from all WMs and WM facilities, analyse the composition of offences in accordance with WM legislation and the Metaverse Magna Carta itself, form a chain of "territorial responsibility" and will compile a list of participants in the proceedings. For example, if an electronic offence relates to national "analog" legislation, then such an offence will be considered within the national jurisdiction. In the event that an electronic offence relates to CfM or SM jurisdictions of different Metaverses, such offence will be considered by the Chamber of the Grand Digital Court of WM. At this stage of the formation of WM and its Metaverse Magna Carta, national legislation needs to be reconfigured or modernised to ensure legal compatibility and the functioning of the emerging Metaverse in order to streamline public relations and activities in the field of information technologies.

The rules and norms of behaviour in WM are still created in accordance with the projection of the physical world and are corporate in nature. However, there is a tendency to migrate and transfer the norms of public morality to the Metaverse by modelling cosmopolitan digital social relations in the absence of clear attributes of the electronic state and state structure of the Metaverse. The development of global digital Metaverse legislation will give impetus to the modernisation of national legislations.

The model of digital jurisdiction will outline the most important and problematic issues that arise in the process of human evolution and the development of virtual reality technologies, as well as form the basis of digital law for the regulation of social relations in the Metaverse.

The core values and objects of the Metaverse to be protected in a digital jurisdiction are:

1. The trust and reputation that is formed by each Metaverse entity and object from the moment it is registered in the Metaverse using blockchain technology.

2. Integrity, reliability and validity of identification data used to identify individuals and legal entities, other subjects and objects in the Metaverse:

biometric identification of individuals, as a particularly valuable and unique attribute or access code to the Metaverse;

IoT identification data (Universal Identifiers of Objects of Identification Systems (OIDs), Electronic Product Code (EPC), Universal Unique Identifier (UUID) and International Mobile Identifier (IMEI));

AI, AAI, and ASI identification data (electronic certificates of quantum cryptographic systems that will protect the AI core from external attacks);

identification data of other types of objects.

3. Intellectual property rights and ownership of non-property electronic assets in the Metaverse.

4. Information security and cybersecurity.

The creation of the Magna Carta Metaverse requires the involvement of a large number of specialists in the field of law and modern digital technologies, as well as specialists who will conduct interdisciplinary research in many areas.

The Magna Carta Metaverse project is a project that will be developed on the initiative and participation of organisations, Metaverse corporations and research institutes, as well as leading Metaverse specialists working in the field of law and modern electronic technologies.

5.4.2. Principles of functioning of digital jurisdiction.

The principle of extraterritoriality.

Digital jurisdiction applies to all digital events, transactions, transactions, or information processes, regardless of the physical location of their participants or the technical location of the servers (Wang, 2024) [1] ; if such an event creates legal consequences, affects the rights, duties or interests of persons in the legal field of the state, it falls under the scope of national legislation (Yang, 2024)[2] (Figure 67). This principle ensures the ability of the state to protect its citizens, digital residents and institutions in global cyberspace by overcoming the limitations of physical territory (Hildebrandt, 2013; Li, 2022)[3]. It forms the basis for the legal recognition of cross-border actions in blockchain networks, Metaverse, and cloud environments, defining that the digital space is an extension of the national legal system, where the norms of the Constitution, international treaties, and the principles of digital sovereignty apply (Ryngaert, 2023; Sullivan & Tyson, 2023)[4].

The principle of legal identity.

Each participant in digital legal relations has a confirmed digital identity (Sullivan, 2018) [5], which is recognised as equivalent to personal presence and ensures its legal status in all forms of digital interaction (Vardanyan et al., 2024) (Sedlmeir et al., 2021)[6,7]. Digital identity is created through a system of multi-level authentication, digital signatures, biometric parameters and cryptographic keys that guarantee the uniqueness and inviolability of personal data. It has legal force for concluding contracts, participating in court proceedings, filing applications and receiving administrative services (Sullivan, 2023) [8] . Legal identity acts as the foundation of digital citizenship, allows for the establishment of responsibility for actions in cyberspace, prevents fraud and ensures verification of the legitimacy of digital transactions (Michałkiewicz-Kądziela & Milczarek, 2022)[9]. Its presence is a prerequisite for the legitimacy of any actions within the digital jurisdiction of the State.

---

1 Wang, Y. (2024). Do not go gentle into that good night: The European Union's and China's different approaches to the extraterritorial application of artificial intelligence laws and regulations. *Computer Law & Security Review, 53*, 105965. https://doi.org/10.1016/j.clsr.2024.105965.

2 Yang, Y. (2024). Analysis on the extraterritorial expansion and conflict of digital prescriptive jurisdiction. *Dispute Settlement*. https://doi.org/10.12677/ds.2024.101017

3 Li, K. (2022). Reconceiving extraterritorial jurisdiction. *German Yearbook of International Law*. https://doi.org/10.5771/9783748933212

4 Ryngaert, C. (2023). Extraterritorial enforcement jurisdiction in cyberspace: Normative shifts. *German Law Journal, 24*, 537–550. https://doi.org/10.1017/glj.2023.24

5 Sullivan, C., & Tyson, S. (2023). A global digital identity for all: The next evolution. *Policy Design and Practice, 6*(4), 433–445. https://doi.org/10.1080/25741292.2023.2267867.

6 Sullivan, C. (2018). Digital identity—From emergent legal concept to new reality. *Computer Law & Security Review, 34*(4), 723–731. https://doi.org/10.1016/j.clsr.2018.05.015.

7 Vardanyan, L., Hamuľák, O., & Kocharyan, H. (2024). Fragmented identities: Legal challenges of digital identity, integrity, and informational self-determination. *European Studies, 11*, 105–121. https://doi.org/10.2478/eustu-2024-0005.

8 Sullivan, C. (2023). Digital identity as an international legal concept – New disturbing developments. *Georgetown Journal of International Affairs, 24*, 29–35. https://doi.org/10.1353/gia.2023.a897698.

9 Michałkiewicz-Kądziela, E., & Milczarek, E. (2022). Legal boundaries of digital identity creation. *Internet Policy Review, 11*(1). https://doi.org/10.14763/2022.1.1614.

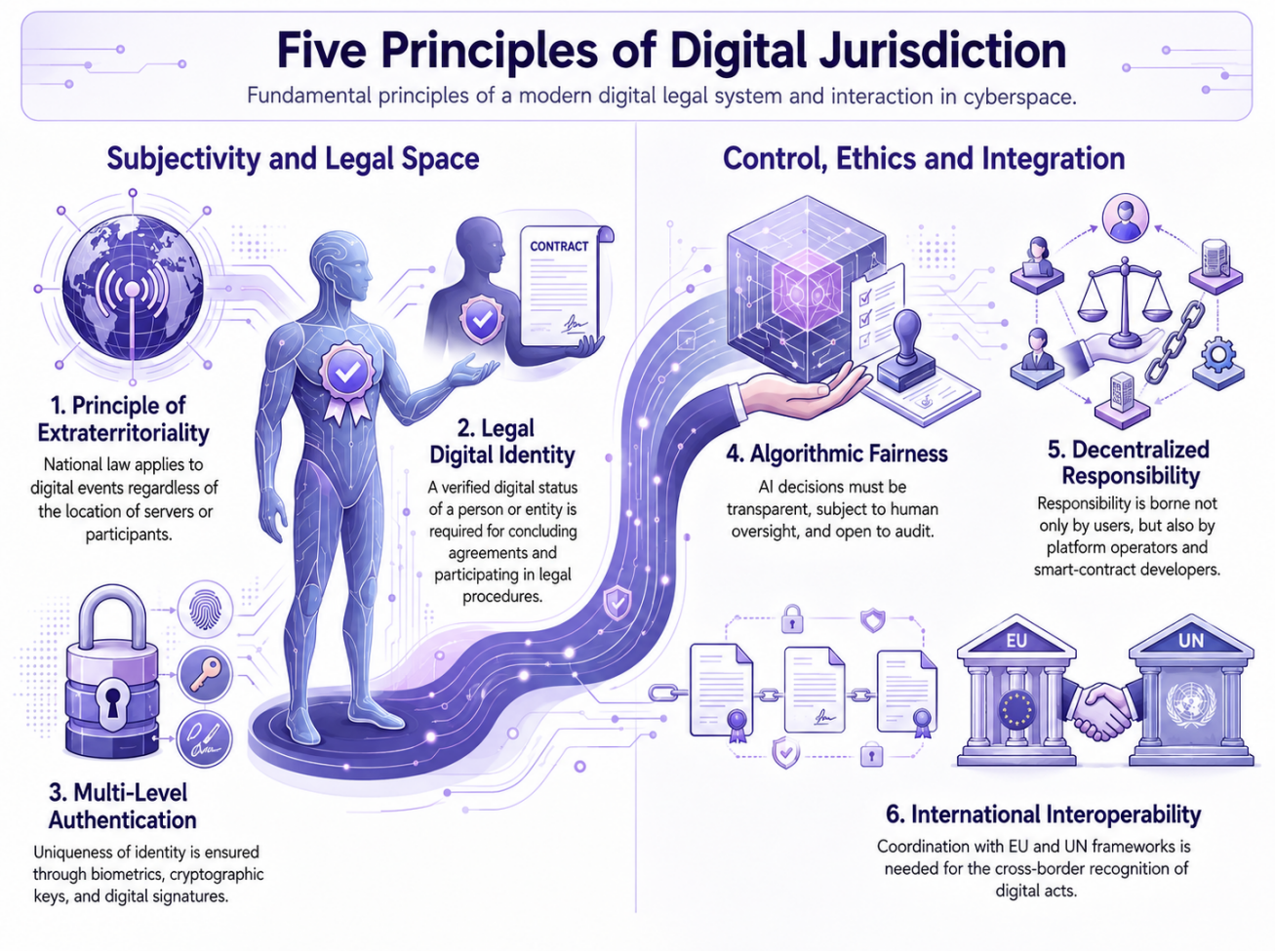


Figure 67. Five principles of digital jurisdiction

The principle of algorithmic justice.

Decisions made with the participation of artificial intelligence should be transparent, verifiable, human-controlled, and comply with the principles of legality, proportionality, and protection of human rights (Sachan & Liu, 2024)[1]. Within a digital jurisdiction, algorithmic justice includes the ability to audit decision-making models (Chiao, 2019)[2], the public availability of descriptions of the logic of the functioning of systems, the provision of the possibility of appealing the results generated with the participation of AI, and the mandatory intervention of a person in cases with legal consequences (Rong, 2024)[3]. The state ensures that the use of artificial intelligence in legal processes does not lead to discrimination, distortion of facts, or manipulation of evidence, and all algorithmic tools are independently certified for ethical and legal compliance (Lee et al., 2019)[4].

1 Sachan, S., & Liu, X. (2024). Blockchain-based auditing of legal decisions supported by explainable AI and generative AI tools. *Engineering Applications of Artificial Intelligence, 129*, 107666. https://doi.org/10.1016/j.engappai.2023.107666.

2 Chiao, V. (2019). Fairness, accountability and transparency: Notes on algorithmic decision-making in criminal justice. *International Journal of Law in Context, 15*(2), 126–139. https://doi.org/10.1017/S1744552319000077

3 Rong, S. (2024). A legal study of transparency and fairness in algorithm-driven legal decision support systems. *Applied Mathematics and Nonlinear Sciences, 9*. https://doi.org/10.2478/amns-2024-3386

4 Lee, M., Jain, A., Cha, H., Ojha, S., & Kusbit, D. (2019). Procedural justice in algorithmic fairness. *Proceedings of the ACM on Human-Computer Interaction, 3*, 1–26. https://doi.org/10.1145/3359284.

The principle of decentralised responsibility.

Digital law entities are obliged to ensure that their actions comply with the norms of national, international and ethical law, regardless of the technical form of their implementation or the location of the technological infrastructure (Napieralska & Kępczyński, 2024).[1] This principle implies that responsibility for the consequences of digital activities lies not only with individuals or legal entities, but also with platform operators, algorithm owners, smart contract developers, administrators of decentralised systems, and other AI participants in the digital ecosystem (Dwivedi et al., 2021)[2]. Decentralised responsibility means the collective obligation of actors to ensure the transparency, reliability and security of transactions, to prevent human rights violations, cybercrimes, manipulation or creating risks to the digital sovereignty of the state (Truong et al., 2021)[3].

The principle of interoperability.

The digital jurisdiction of the State is consistent with the legal regimes of the EU, the Council of Europe, the UN, ISO and other international institutions, providing the possibility of cross-border recognition of electronic documents, digital signatures and decisions of judicial or arbitral authorities (Djuraev et al., 2025)[4]. Interoperability encompasses the technical, legal, and ethical interoperability of systems (Jimenez-Gomez, 2012). [5]This principle creates the basis for the integration of the State's digital jurisdiction into the global digital legal order, where the mutual recognition of data and decisions guarantees trust, transparency, and efficiency of legal processes (Malik et al., 2023)[6].

1 Napieralska, A., & Kępczyński, P. (2024). Redefining accountability: Navigating legal challenges of participant liability in decentralized autonomous organizations. *arXiv*. https://doi.org/10.48550/arXiv.2408.04717.

2 Dwivedi, V., Pattanaik, V., Deval, V., Dixit, A., Norta, A., & Draheim, D. (2021). Legally Enforceable Smart-Contract Languages. *ACM Computing Surveys (CSUR)*, 54, 1-34. https://doi.org/10.1145/3453475

3 Truong, N., Lee, G. M., Sun, K., Guitton, F., & Guo, Y. (2021). A blockchain-based trust system for decentralised applications: When trustless needs trust. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2021.05.025.

5 Djuraev, I., Baratov, A., Khujayev, S., Yakubova, I., Rakhmonova, M., Mukumov, B., & Abdurakhmanova, N. (2025). The impact of digitization on legal systems in developing countries. *Qubahan Academic Journal*. https://doi.org/10.48161/qaj.v5n1a1246

5 Jimenez-Gomez, C. (2012). *Implementing interoperability in e-justice's criminal area*.

6Malik, V., Mittal, R., Mavaluru, D., Narapureddy, B., Goyal, S., Martin, R., Srinivasan, K., & Mittal, A. (2023). Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks. *IEEE Access, 11*, 70110–70131. https://doi.org/10.1109/ACCESS.2023.329352.

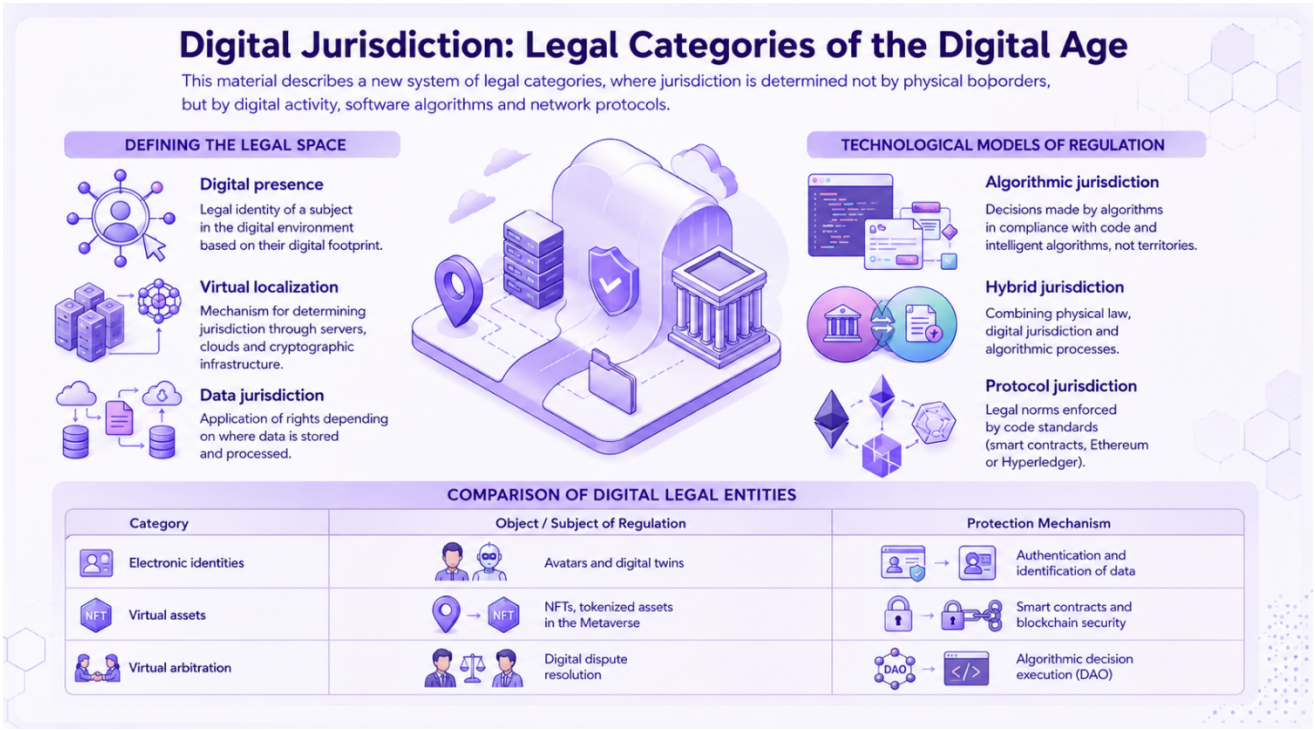


Figure 68. Digital jurisdiction – legal categories of the digital age.

5.4.3. Key categories of digital jurisdiction.

Digital presence is an extended legal category of modern digital law, which means a legally significant fact of activity of a subject or object of legal relations in the digital environment, regardless of its physical location. It covers both direct participation in transactions and indirect forms of activity — the creation of digital profiles, the functioning of avatars (Raposo, 2024)[1], the use of smart devices and sensor systems, presence in Metaverses or XR platforms. Digital presence becomes the basis for acquiring rights and obligations, determines the possibility of legal liability, and is a legally significant element in the process of establishing digital jurisdiction (Noval & Maaruf, 2024)[2]. It takes into account not only the fact, but also the duration, intensity and nature of digital activity, and in the case of autonomous agents, algorithmic behaviour, which is equated to the actions of individuals or legal entities (Barfield & Williams, 2018)[3].

Virtual localisation is an extended legal category that means a mechanism for determining whether digital transactions, data, or transactions belong to a specific jurisdiction by means of cryptographic and protocol fixation. It takes into account the geography of servers, the structure of blockchain networks, technical protocols for transmitting information and certification standards, and other AI factors that determine the conditional "location" of a digital event. Virtual localisation allows you to tie actions in a virtual environment to a specific legal system, even if they are carried out in a decentralised or cross-border format. It provides legal certainty for electronic

1 Raposo, V. (2024). Beyond pixels and profiles: Unveiling the legal identity of avatars in the metaverse. *Interactive Entertainment Law Revie, 7*(1), 22–45. https://doi.org/10.4337/ielr.2024.02.04

2 Noval, S., & Maaruf, I. (2024). Toward a comprehensive cyber law framework: Assessing avatar legal liability. *China and WTO Review*, *10*(1), 161–182. https://doi.org/10.52152/cwr.2024.10.1.07

3 Barfield, W., & Williams, A. (2018). The law of virtual reality and increasingly smart virtual avatars. In *Research handbook on the law of virtual and augmented reality* (pp. 2–43). https://doi.org/10.4337/9781786438591.00008

transactions, eliminates anonymous evasion of legal regimes and creates conditions for the integration of state and international standards into a single e-justice system.

Algorithmic location is an extended legal category that defines jurisdiction not by physical territory, but by the boundaries of which digital network, protocol, or blockchain a transaction, action, or transaction is carried out (Watters, 2023), functioning as a substitute for geographical "territories" when the geographical jurisdiction is not able to fully regulate digital legal relations (Musthafa et al., 2024)[1]. Algorithmic location provides prerequisites for the formation of new models of digital arbitrage, the recognition of smart contract solutions, and the formation of digital sovereignty of communities (De Filippi & Hassan, 2016)[2].

Multi-jurisdictional process is an extended legal category that covers a set of legal relations that simultaneously fall under the scope of several legal systems in the digital environment. This applies to situations when a transaction or transaction is carried out in global blockchain networks, Metaverse spaces, or cloud infrastructures, and their consequences are simultaneously regulated by different national and supranational legal regimes. It requires the prevention of legal conflicts, prioritisation of the application of a particular system of law and creation of mechanisms for joint resolution of disputes between subjects of different jurisdictions.

Cross-border digital legal personality is an extended category of legal status, which means the acquisition by individuals or legal entities of rights and obligations simultaneously in several digital legal orders. It takes into account the participation of entities in cross-border blockchain networks (Garcia-Teruel & Simón-Moreno, 2021),[3] e-ecosystems, global data clouds, and decentralised autonomous organisations (DAOs), where legal consequences are formed outside the classical territorial borders of states. Such status implies simultaneous subordination to the norms of different jurisdictions, the recognition of electronic identities and transactions in several legal systems, as well as the creation of mechanisms to prevent conflicts and double liability (Glasze et al., 2022)[4]. Cross-border digital legal personality forms the basis for the global interoperability of digital law and contributes to the harmonisation of legal regimes in the areas of data, contracts, and digital identity (Quinn, 2021)[5].

Data jurisdiction is an extended legal regime that determines the application of the law depending on the place of storage, processing, transmission or origin of data, including in the context of distributed ledgers and multi-tier cloud systems. It covers the issues of control over cross-border data movement, the application of legal regulations to global data centres, liability for leaks or manipulation of information, as well as ensuring

1 Musthafa, A., Putri, R., Farizki, A., & Alma, S. (2024). Lex cryptographia: Legal extensions to smart contract breaches and governance in blockchain systems. *Journal of Legal Reform Studies, 4*(2), 173–202. https://doi.org/10.19184/jkph.v4i2.53366

2 De Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday, 21*(12). https://doi.org/10.5210/fm.v21i12.7113

3 Garcia-Teruel, R., & Simón-Moreno, H. (2021). The digital tokenization of property rights: A comparative perspective. *Computer Law & Security Review, 41*, 105543. https://doi.org/10.1016/j.clsr.2021.10554

4 Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2022). Contested spatialities of digital sovereignty. *Geopolitics, 28*(3), 919–958. https://doi.org/10.1080/14650045.2022.2050070.

5 Quinn, J. (2021). Geo-location technology: Restricting access to online content without illegitimate extraterritorial effects. *International Data Privacy Law*, *11(4),* 312–326. https://doi.org/10.1093/idpl/ipab016

the digital sovereignty of the state. Data jurisdiction takes into account both technical parameters — geolocation of servers, traffic routing, encryption algorithms — and legal factors: national legislation, international treaties, localisation and data exchange policy. Its purpose is to guarantee the protection of the rights of subjects, the transparency of processing and the compatibility of national regimes with international standards, in particular in the field of GDPR, ISO/IEC and free data flow agreements.

Virtual arbitration forum is an extended legal construct that means a specially created digital space or protocol within which the parties agree to resolve disputes regardless of geographical location and national jurisdiction (Okezie, 2024; Wiegandt, 2022)[1,2]. Such a forum can function as a blockchain platform, a decentralised autonomous organisation (DAO), or a smart contract system that automatically enforces arbitral decisions based on algorithmic rules (Gabuthy, 2023; Aouidef et al., 2021)[3, 4]. A virtual arbitration forum guarantees neutrality, transparency, and efficiency in the resolution of disputes, allows the use of combined methods of proof — digital traces, blockchain records, immersive reconstructions — and provides legal certainty and the formation of global trust in cross-border digital relations (Gronic, 2023)[5].

A hybrid jurisdiction is an integrated legal regime that combines elements of physical, digital, and algorithmic jurisdiction to resolve complex disputes (Gronic, 2023)[6]. It is used in cases where a single legal conflict encompasses physical actions, digital transactions, and algorithmic processes that interact within a single legal event at the same time (Atiyah et al., 2024)[7]. An example is a situation where a transaction is concluded in a virtual environment, confirmed by a smart contract on the blockchain, and has consequences in the physical world (supply of goods or provision of a service) (Szabo et al., 2024)[8]. A hybrid jurisdiction ensures uniformity of law enforcement, prevents collisions, and allows the use of mixed proof mechanisms: from classic documents to blockchain records and data from the Metaverse. It also provides for the creation of specialised arbitration and court instances capable of integrating different levels of evidence and providing comprehensive technical and legal dispute resolution.

Protocol jurisdiction is a legal regime determined not by the territory, but by a standard or technical protocol on the basis of which a digital service or network operates. It establishes that the application of legal norms depends on the chosen architecture of the communication protocol: for example, if a transaction is made through Ethereum or

1 Chevalier, M. (2021). From smart contract litigation to blockchain arbitration: A new decentralized approach leading towards the blockchain arbitral order. *Journal of International Dispute Settlement, 12*(4), 558–584. https://doi.org/10.1093/jnlids/idab025

2 Okezie, P. (2024). Resolving smart contract disputes through blockchain arbitration. *Arbitration: The International Journal of Arbitration, Mediation and Dispute Management*, *90*(1), 111–125. https://doi.org/10.54648/amdm2024013.

3 Wiegandt, D. (2022). Blockchain and smart contracts and the role of arbitration. *Journal of International Arbitration*, *39*(4), 543–568.https://doi.org/10.54648/joia2022029.

4 Gabuthy, Y. (2023). Blockchain-based dispute resolution: Insights and challenges. *Games, 14*(3), 34. https://doi.org/10.3390/g14030034.

5 Aouidef, Y., Ast, F., & Deffains, B. (2021). Decentralized justice: A comparative analysis of blockchain online dispute resolution projects. *Frontiers in Blockchain, 4*, 1–8. https://doi.org/10.3389/fbloc.2021.56455.

6 Gronic, I. (2023). Transforming digital dispute resolution in India. *RUDN Journal of Law, 27*(4), 1113–1124. https://doi.org/10.22363/2313-2337-2023-27-4-1113-1124.

7 Atiyah, G., Ibrahim, A., & Jasim, A. (2024). Enforcement of smart contracts in cross-jurisdictional transactions. *International Journal of Law and Management*, *66*(5), 612–628. https://doi.org/10.1108/ijlma-06-2024-0220.

8 Szabo, J., Bernard, C., & Philip, L. (2024). Legal implications and challenges of blockchain technology and smart contracts. *Computer Life*, *4*(2), 45–58. https://doi.org/10.54097/ztn2w848.

Hyperledger, it is these protocols that set the basic legal framework for the fulfilment of obligations. Protocol jurisdiction takes into account the specifics of network standards — ISO, W3C, TCP/IP, blockchain protocols — their interoperability and security rules, and also forms the basis for resolving disputes within a specific technological environment.

Digital identities and avatars are a legal category that determines the legal status of digital copies of a person (avatars, digital identities, digital humanoids) capable of acting independently in the Metaverse (Global et al., 2024)[1]. It provides for granting them partial legal capacity, determining the limits of responsibility for actions performed on behalf of the owner or autonomously, establishing the procedure for authenticating identification data and ensuring the legitimacy of their existence in the system of digital jurisdiction.

Virtual non-property assets are a legal category that covers digital objects in the Metaverse (virtual land plots, NFTs, digital content) that do not have a tangible form, but are recognised as valuable and subject to legal regulation. It defines the rules of ownership, use, disposal, establishes mechanisms for confirming ownership and protecting against misappropriation through smart contracts and blockchain registries.

Numerical offences are a special legal category that records actions that are illegal in nature exclusively in the digital environment (for example, manipulation of digital avatars, NFT fraud, abuse of immersive technologies, and other actions that have no analogues in physical space). It provides for distancing from analog offences and establishing new standards of legal qualification and liability within digital jurisdiction.

Identity data is a legal category that regulates the use of identification and personal data to create, authenticate, and operate virtual avatars, digital twins, and electronic humanoids in the Metaverse. It involves the use of biometric parameters, IoT identifiers, and quantum cryptographic certificates to ensure legal security, authenticity, and trust in digital legal relationships (Svantesson, 2013)[2].

The digital justice regime is an extended legal category that encompasses judicial and quasi-judicial mechanisms for the administration of justice in the Metaverse: from local virtual tribunals to supranational arbitration chambers. It defines the rules of jurisdictional jurisdiction, procedural status of participants, guarantees of due process, and algorithmic mechanisms for appealing decisions in a digital or mixed enforcement environment (Figure 69).

1 Kostenko, O., Dniprov, O., Zhuravlov, D., & RS Global. (2024). Metaverse: Ensuring legal recognition of avatars and electronic personalities through a cross-border personalized ID-code. *International Journal of Innovative Technologies in Social Science, 2(42)*, 1–12. https://doi.org/10.31435/rsglobal_ijitss/30062024/8141

2 Svantesson, D. J. B. (2013). A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law, 3*(4), 278–286. https://doi.org/10.1093/idpl/ipt027.

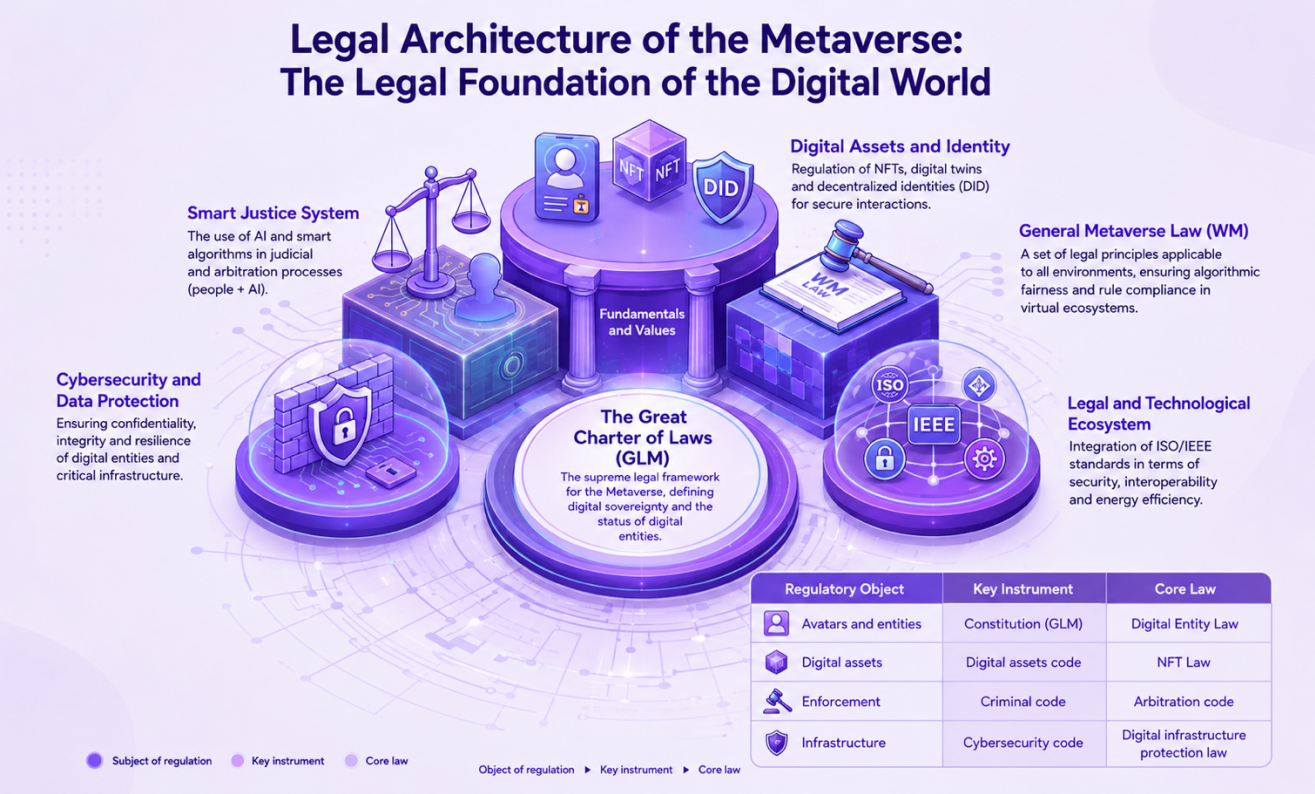


Figure 69. The legal foundation of the digital world.

5.4.4. Legal architecture of digital jurisdiction.

The Metaverse Constitution (Magna Carta, GLM) is a basic metalegal document that defines the principles of digital sovereignty, guarantees the rights, freedoms, and obligations of users, and regulates the legal status of algorithmic agents, autonomous systems, and digital avatars. The Constitution sets the structure of digital governance, arbitration procedures, and coordination of interstate digital platforms, ensuring stability and fairness in all dimensions of the Metaverse (Bibri & Allam, 2022)[1].

GLM acts as the architectural core of the Metaverse digital jurisdiction, forming it as the Meta-Legal Operating System — a dynamic multi-level platform for legal management of digital relations. The main functions of GLM are: ensuring compatibility between national and algorithmic systems of law; creation of a single semantic database of digital norms (Smart Law Ontology); maintaining the ethical-centric legitimacy of digital processes; creating conditions for global interstate cooperation in the field of e-justice.

The general norms and structure of the laws of the Magna Carta define the principles of digital rule-making, methods of harmonisation between national, corporate and global legal standards, as well as establish the procedure for creating, updating and validating electronic norms.

Metaverse common law (the legal, institutional, and technological space of the Metaverse) forms a system of precedents, norms of behaviour, and algorithmic justice

1 Bibri, S. E., & Allam, Z. (2022). The metaverse as a virtual form of data-driven smart cities: The ethics of hyper-connectivity, datafication, algorithmization, and platformization of urban society. *Computational Urban Science, 2*, 22. https://doi.org/10.1007/s43762-022-00050-

mechanisms. It establishes the principles of equal access to digital justice, defines algorithms for considering electronic disputes, and standards of conduct in between digital actors and national legal systems, ensuring flexibility, efficiency and fairness in the application of digital law (Watts, 2025; Tan, 2023)[1,2].

The Metaverse Judicial Digital System is a multi-layered digital justice architecture that encompasses digital courts, arbitration protocols, ombuds-agents, and Smart Justice modules. It ensures the fairness and transparency of e-justice, encompassing both fully automated and hybrid litigation processes in which decisions are formed with the participation of artificial intelligence and humans. Within Smart Justice, digital mediation, automated arbitration, and monitoring modules are implemented for enforcement of court decisions, which ensures the effective, reliable and continuous functioning of digital justice in the Metaverse.

The Metaverse Electronic Office Act (E-Office Act) regulates the administrative, procedural, and organisational aspects of managing the activities of electronic entities, defines mechanisms for digital accountability, accounting, and coordination of interaction between institutional agents in the Metaverse (Chen, 2023[3]). In addition, the E-Office Act creates legal framework for the implementation of automated administrative processes, electronic licensing systems, auditing, and control over the activities of algorithmic administrations within the Metaverse (Ryu et al., 2022)[4].

The cross-border interaction regime in the Metaverse establishes the legal framework for data exchange, electronic evidence, inter-jurisdictional arbitration, and digital diplomacy. It defines the procedure for mutual recognition of electronic identifiers, authentication procedures and the use of digital signatures between different jurisdictions, ensuring legal interoperability at the level of data protocols and cross-border smart contracts.

The Metaverse Large Electronic Judicial Code regulates the procedures of e-justice, smart decisions, and AI-based evidentiary analytics. It details the processes of filing and considering electronic claims, automated recording of evidence, algorithmic assessment of the circumstances of the case, and the procedure for making decisions using artificial intelligence systems. The Code defines the standards of digital procedural law, regulates the work of virtual courtrooms, digital juries, and arbitration platforms, as well as establishes rules for electronic appeal and verification of the fairness of smart solutions. Special attention is paid to ensuring transparency, exercising the right to protection and observing the principle of human control in the context of the functioning of mixed digital justice systems Metaverse.

The Metaverse Code of Non-Property Digital Assets regulates the circulation of NFTs, virtual lands, digital works, and data as objects of ownership (Wyczik, 2024)[5]. It

1 Watts, J. (2025). *Law in the metaverse*. https://doi.org/10.5040/9781526530783

2 Tan, A. (2023). Metaverse realities: A journey through governance, legal complexities, and the promise of virtual worlds. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4393422

3 Chen, Z. (2023). Metaverse office: Exploring future teleworking model. *Kybernetes, 53*(6), 2029–2045. https://doi.org/10.1108/K-10-2022-1432.

4 Ryu, J., Son, S., Lee, J., Park, Y., & Park, Y. (2022). Design of secure mutual authentication scheme for metaverse environments using blockchain. *IEEE Access, 10*, 98944–98958. https://doi.org/10.1109/ACCESS.2022.3206457.

5 Wyczik, J. (2024). The rise of the metaverse: Tethering effect and intellectual property of crypto tokens. *Journal of Intellectual Property Law & Practice*. https://doi.org/10.1093/jiplp/jpad12

defines the legal status of intangible assets, the procedure for their registration, confirmation of authorship, and the transfer of rights in digital form. The Code establishes the rules for the circulation of tokenised intellectual property, the conditions for the creation and use of digital certificates of ownership, as well as mechanisms for resolving disputes. Particular [1] attention is paid to the inheritance of non-property electronic assets, their preservation in decentralised ledgers, as well as protection against manipulation and falsification of metadata. Thus, the Code creates a legal basis for the legitimate functioning of the digital property economy in the Metaverse (Limongelli & Sposini, 2025)[2].

The Metaverse Criminal Digital Code defines the types of crimes in the field of cyberspace, establishes responsibility for the actions of algorithmic agents, and ensures the digital security of the individual. It establishes levels of responsibility between a person, a developer and an autonomous system, defines mechanisms for electronic investigation, digital forensics, and evidentiary verification (Sallavaci, 2020; Casino et al., 2022)[3, 4]. In addition, the Code provides for a system of digital rehabilitation, guarantees of protection of the rights of victims of cybercrimes, and principles of humane treatment in the context of digital justice in the Metaverse (Kostenko et al., 2023; Arnell & Faturoti, 2023)[5].

The Metaverse Cybersecurity Code provides legal regimes for cyber defence, incident response, and protection of critical digital infrastructure. It defines the principles of cyber resilience, risk management, and continuity of digital operations, establishes standards for responding to cyberattacks, and the procedure for coordination between public and private entities in the field of cybersecurity (Fiaz et al., 2024)[6]. The Code provides for the creation of an early warning system, the introduction of a legal regime for cyber monitoring, the audit of the security of critical facilities, and the introduction of interaction protocols in case of emergency digital threats (Srinivas et al., 2019)[7].

The Metaverse Code of Fundamental Technical Regulations defines basic standards for security, certification, cryptography, cybersecurity, and interoperability. The Code regulates the application of ISO, IEEE, ITU and other internationally recognised standards, integrating them into a single Metaverse techno-legal ecosystem (Figure 70).

---

1 García, R., Cediel, A., Teixidó, M., & Gil, R. (2022). Semantics and non-fungible tokens for copyright management on the metaverse and beyond. *ACM Transactions on Multimedia Computing, Communications, and Applications, 20*(1), 1–20. https://doi.org/10.1145/3585387

2 Limongelli, R., & Sposini, L. (2025). The (virtual) battle for intellectual property rights in the metaverse: The case of copyright, trademarks and the NFT technology. *Metaverse*. https://doi.org/10.54517/m30

3 Sallavaci, O. (2020). Rethinking criminal justice in cyberspace: The EU e-evidence framework as a new model of cross-border cooperation in criminal matters. In *Digital forensics and cyber crime* (pp. 1–58). https://doi.org/10.1007/978-3-030-50613-1_1

4 Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *arXiv*. https://doi.org/10.48550/arXiv.2205.12911

5 Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime – Why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology, 37*(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888

6 Fiaz, F., Sajjad, S., Iqbal, Z., Yousaf, M., & Muhammad, Z. (2024). MetaSSI: A framework for personal data protection, enhanced cybersecurity and privacy in metaverse virtual reality platforms. *Future Internet, 16*(5), 176. https://doi.org/10.3390/fi16050176

7 Srinivas, J., Das, A., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063.

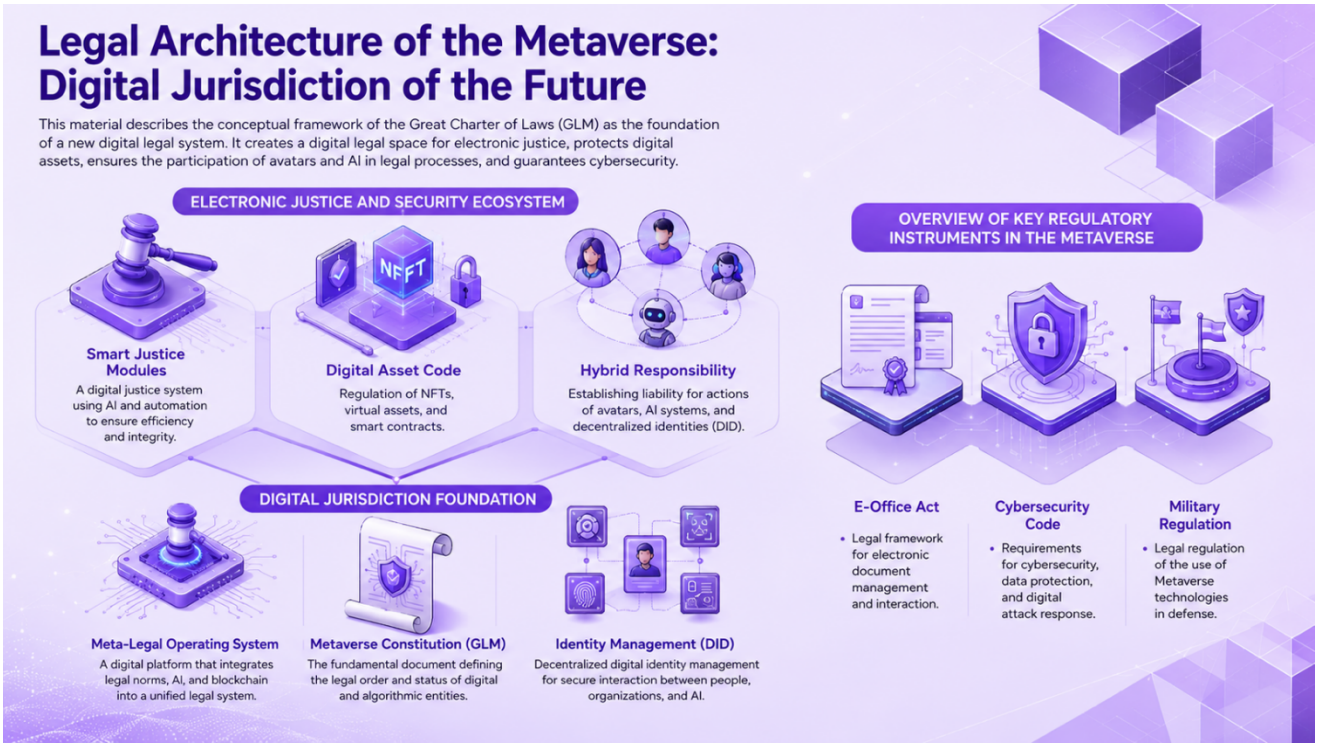


Figure 70. Metaverse: the digital jurisdiction of the future.

The Metaverse Identity Management Certificate defines the procedure for creating, verifying, and protecting digital identities (Kostenko, 2020; Akramov et al., 2024).[1] [2]It establishes procedures for digital authentication, access rights management, and delegation of identification authority within a digital jurisdiction (Kostenko, 2021c; Kostenko, 2021b)[3]. The certificate also provides mechanisms for personal data protection, prevention of counterfeiting, the use of decentralised identifiers (DIDs) and verified credentials (VCs), ensuring secure interaction between a person, an organisation, and algorithmic actors in a Metaverse environment (Chen, 2025; Kostenko, 2021c)[4,5].

The Metaverse Military Regulations establish the norms of digital defence, algorithmic command, and humanitarian law in the context of cyber conflicts. It defines the principles of the use of cyber forces, the procedure for interaction between military and civilian digital structures, as well as security standards during virtual operations. The regulations regulate the procedures for managing autonomous defence systems, monitoring the use of artificial intelligence for military purposes, and rules for conducting information operations and protecting civilians in the Metaverse.

1 Kostenko, O. (2020). Identification data management: Legal regulation and classification. *Scientific Journal of Polonia University, 43*(6), 198–203. https://doi.org/10.23856/4325

2 Akramov, A., Rakhmonkulova, N., Khazratkulov, O., Inamdjanova, E., Imamalieva, D., Tuychieva, S., Ibodullaev, S., Ergashev, A., Khamidov, S., & Rustamova, N. (2024). The impact of digitalization in inheritance law. *Qubahan Academic Journal*. https://doi.org/10.48161/qaj.v4n3a863.

3 Kostenko, O. (2021b). Management of identification data: Legal regulation and classification. *Young Scientist, 3*(91), 90–94. https://doi.org/10.32839/2304-5809/2021-3-91-21

4 Chen, Z. (2025). Building a legal framework for the metaverse: Digital identity, NFT property rights, and global legal structures. *Digital Society & Virtual Governance***.** https://doi.org/10.6914/dsvg.010104.

5 Kostenko, O. (2021c). Paradigms of identity data management in the light of the development of IoT devices and artificial intelligence. *Amparo, 3*, 42–47. https://doi.org/10.26661/2616-9444-2021-3-0

5.4.5. Regulatory mechanisms.

Legitimation of digital evidence.

Electronic documents, blockchain records, digital traces, data from the Metaverse, telemetry signals, biometric indicators, records of sensor devices, and the results of autonomous systems are recognised as admissible evidence, provided that three key criteria are met: authenticity, integrity, and legal suitability.

The category of digital evidence also includes digital evidence from the Metaverse, audio and video data of XR environments, machine logs of autonomous systems, cryptographic log files and the results of algorithmic analysis of events. The procedure for their legitimation is determined by a special protocol of the Digital Code, which provides the possibility of filing, verifying and challenging such evidence within the framework of algorithmic jurisdiction.

*Virtual transactions***.**

Entering into transactions in the digital environment — including smart contracts, DAO solutions, algorithmic commitments, digital memorandums, and automated transaction scenarios — is recognised as equivalent to offline transactions, subject to compliance with a set of requirements defined by the Digital Code. The category of virtual transactions includes not only economic transactions, but also DAO management decisions, legally significant actions in metaverses, algorithmic agreements between artificial agents, and human-machine interactions that generate obligations or changes in legal status. All such actions are regulated by the principle of lex algorithmica, according to which digital codes acquire legal significance provided that they are certified and integrated into the system of digital jurisdiction.

Responsibility in a multi-jurisdictional environment.

Participants in digital legal relations bear combined, multi-level responsibility depending on their digital affiliation, jurisdictional status and the nature of the actions committed. Such responsibility includes three interrelated levels:

- primary (national) responsibility is regulated by the norms of the state of registration of the digital entity or the jurisdiction within which its keys, servers or other means of authentication are located;
- secondary (cross-border) liability is applied in cases of impact on the rights of foreign citizens, assets or digital platforms, taking into account the provisions of international treaties, digital conventions and the principles of mutual recognition;
- Algorithmic liability — rests with developers or owners of autonomous systems whose code or artificial intelligence has caused harm, loss, or infringement of rights.

In addition, the principle of extraterritorial effect of digital norms is provided, according to which national legislation can apply to digital actions that have consequences for citizens or national infrastructure, regardless of the place where the algorithm is executed or data is stored.

Algorithmic jurisdiction.

In cases arising from the application of smart contracts, blockchain protocols, autonomous agents or hybrid artificial intelligence systems, the logic of the code, the consensus mechanism and the digital trace of the execution of the algorithm are decisive.

Such disputes are considered within a special legal field — algorithmic jurisdiction, based on the principles of techno-legal neutrality, transparency and compliance with international ethical standards. Algorithmic jurisdiction includes three main levels:

- technical level — fixation, auditing, and reproduction of algorithmic actions in the blockchain, verification of digital signatures, hashids, and transaction logs;
- legal level — legal interpretation of the algorithmic code, its equivalence to traditional norms and determination of the moment of occurrence of legal consequences;
- The ethical level is the assessment of decisions of autonomous systems for discrimination, opacity, or violation of the principle of human control.

Digital legal audit. Each digital system that affects the rights of individuals, processes personal or behavioural data, makes decisions based on algorithms or carries out automated management, is subject to periodic comprehensive legal audits. The audit is carried out by an interdisciplinary commission with the participation of lawyers, technical specialists, ethicists, cybersecurity auditors and members of the public. The audit procedure includes the following stages: risk identification, techno-legal review, ethical assessment (human-in-the-loop), assessment of cyber resilience and security, public reporting, etc.

The results of the digital legal audit are published in the National Register of Audit Opinions, which ensures transparency, accountability and the possibility of independent verification. The detected violations may be the basis for the suspension of the algorithm or the application of regulatory sanctions. Such a system guarantees the sustainable compliance of technologies with the principles of ethics, transparency, cyber resilience and the rule of law.

Institutional Architecture.

The National Digital Jurisdiction Commission is the central coordinating body of digital statehood authorised to ensure the systematic implementation, consistent interpretation and proper application of the norms of digital jurisdiction within the national legal space. The Commission performs the functions of strategic management of the digital legal order, coordinates the activities of public authorities, judicial institutions, regulatory structures and private digital platforms in the field of electronic governance. Its powers include: development and examination of draft regulations in the field of digital jurisdiction; certification and monitoring of the security of national digital infrastructures; audit of cross-border digital transactions and data exchange protocols; overseeing compliance with the principles of digital ethics, human rights and cyber sovereignty. The Commission forms and implements the National Digital Jurisdiction Strategy, coordinates state participation in international digital initiatives, and provides feedback between government, civil society and digital actors through open e-consultation platforms. In addition, the Commission acts as a national centre for arbitration mediation in cases arising between citizens, state systems, business entities and algorithmic agents within the digital jurisdiction.

Transnational Digital Arbitration is a new generation international institution created as an independent judicial platform for resolving disputes in the cross-border digital space. Its architecture is built on blockchain technology, which ensures full transparency, openness and the impossibility of external interference in the decision-

making process. Arbitration functions as a digital court with global jurisdiction over disputes arising from the use of smart contracts, DAO agreements, crypto assets, NFT rights, cyber incidents, and algorithmic violations. Its activities are based on the principles of techno-legal neutrality, digital integrity, and automated legitimation of decisions. The Arbitration consists of international expert judges, certified ethical AI models, and representatives of digital states. Such a hybrid structure provides a balance between human competence, algorithmic impartiality and digital sovereignty of the participants in the process.

Digital ombudsmen are independent agents operating in the system of digital jurisdiction in order to ensure the protection of human rights in the digital environment. They function in two formats: human ombudsmen — represent the interests of users in legal procedures; algorithmic e-ombudsmen — work in real time, monitor potential violations of digital rights and generate preventive recommendations.

The Digital Prosecutor's Office and AI supervisory authorities are specialised institutions responsible for detecting, investigating, and prosecuting digital rights violations, data misuse, cybercrimes, and misconduct by artificial agents. They operate on the basis of open algorithmic law, use their own analytical systems to identify risks in digital transactions, conduct forensic examinations, and coordinate with national and international law enforcement structures.

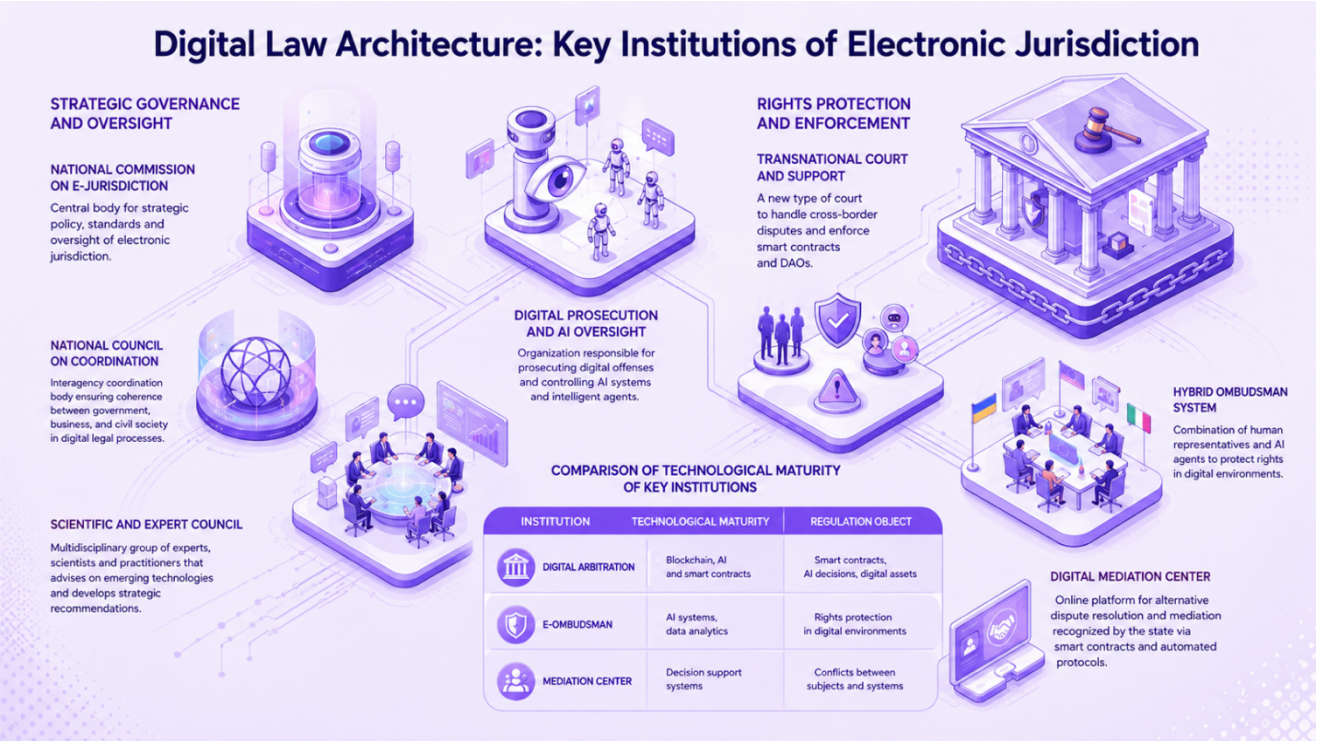


Figure 71. Key institutions of digital law

The Scientific and Expert Council on Digital Technologies and Law is a permanent interdisciplinary body that provides expertise, forecasting and development of strategies for the digital transformation of the legal system. It consists of specialists in the field of law, artificial intelligence, ethics, cybersecurity, sociology and philosophy, as well as innovations in the digital sphere (Figure 71).

The International Legal Control Office is an institution that provides audit and supervision over compliance with international digital law standards. The Office monitors the implementation of Transnational Digital Arbitral Awards, coordinates the activities of digital courts, assesses the effectiveness of national digital regulators, and promotes the unification of digital jurisdiction practices on an international scale.

The Center for Digital Mediation and Algorithmic Diplomacy is an institution that combines legal, communication, and technoethical approaches to resolving conflicts between digital states, corporations, DAOs, and users. The Center is engaged in the prevention of crisis situations in cyberspace, organises and conducts negotiations between subjects of digital disputes, as well as develops diplomatic protocols and codes of ethics for algorithmic interactions.

The Academy of Digital Law and Jurisdictional Innovations is an educational and scientific platform for the training of a new generation of specialists — lawyers, designers, experts in digital jurisdiction (e-jurisprudence) and analysts of artificial intelligence law. The Academy implements programs to prepare judges and investigators to work with digital evidence, organises and conducts internships in digital courts, and creates international research laboratories on the future of jurisprudence.

5.4.6. Cross-border regime of digital jurisdiction.

The principle of global compatibility.

The cross-border regime of digital jurisdiction is based on the mutual recognition of digital acts, certificates, smart contracts and court decisions between the states that are parties to international conventions in the field of electronic law. Its goal is to eliminate gaps between national legal regimes and form a single digital space of legal trust. The regime provides for technical interoperability of data, legal harmonisation, and automated exchange of decisions between jurisdictions through a decentralised system of interstate registers.

The cross-border regime of digital jurisdiction is a comprehensive system of harmonisation of digital legal norms, procedures and technical standards between states, corporations and international institutions.

It involves a combination of three interrelated levels of compatibility:

- Technical level — unification of data formats, encryption algorithms, verification protocols and cyber protection (in particular, in accordance with ISO 20022, W3C, ITU, NIST, ETSI standards, etc.).
- The legal level is the harmonisation of legislation in the field of digital signatures, electronic documents, blockchain records, smart contracts, identity management, XR technologies, digital identity, etc.
- The institutional level is the creation of a network of interstate coordination bodies that ensure a common legal policy, monitoring and supervision of its implementation.
- The global interoperability regime is implemented through a decentralised system of interstate registries that enables automated exchange of decisions, certificates, proofs, and transactions between jurisdictions. These registers operate on the principle of multi-level access: public — for open acts, government — for interstate agreements, encrypted — for confidential cases.

- *Algorithm for the recognition and implementation of digital solutions.*

Recognition of court and arbitral awards made within digital jurisdiction is carried out through a multi-level system of digital attestation: verification of the authenticity of the digital signature and smart contract code of the decision; identification of the digital entity against which the decision was issued; automatic entry of the decision into the international register with fixation of date, hashident, and legal status.

After passing the verification procedure, the decision becomes legally binding on the territory of other participants in the cross-border regime without the need for additional court proceedings.

Digital agreements on mutual legal cooperation.

States, corporations, and supranational bodies can enter into digital agreements on joint dispute resolution, evidence sharing, joint cyber incident investigations, and mutual enforcement of judicial acts. Such agreements are stored in the international blockchain register and have the status of cross-border smart contracts, which come into force automatically if certain terms of cooperation are met.

Cross-border digital agreements are the basic tool of international legal partnership between states, corporations, supranational structures and international organisations. They are aimed at coordinating actions in the field of investigating cyber incidents, exchanging digital evidence, settling disputes between entities of different jurisdictions, as well as ensuring mutual recognition of court and arbitration awards.

Digital identity in cross-border space.

For entities operating in several jurisdictions, a Unified Digital Identity System (Global DID) is being introduced, which provides authentication, verification and protection of personal data during cross-border digital transactions and interstate interaction. Global DID is a universal key to access cross-border justice, electronic notary, arbitration and digital mediation services.

Cross-border digital justice protocols.

They determine a special procedure for considering cases with an international element. To ensure technological compatibility and legal certainty in such cases, special procedural standards apply:

- Remote filing of a claim through the electronic platform of the jurisdiction of origin with the authentication of the applicant by means of digital identity;
- The use of quantum keys to encrypt evidence and secure transfer of procedural documents between jurisdictions;
- Conducting court hearings in XR format environments with full fixation of digital data, biometric identifiers and evidentiary materials;
- Automated enforcement of judgments through a decentralised enforcement mechanism integrated into the international digital registry.

These protocols ensure speed, transparency and mutual recognition of legal procedures between states, forming a new level of algorithmic trust in the field of e-justice.

Ethical and security circuit of cross-border interaction.

The digital jurisdiction regime takes into account the issues of digital sovereignty, personal data protection, confidentiality and the prevention of the use of cross-border mechanisms for cyber manipulation or control over individuals. To this end, joint ethics councils, technical committees on cyber resilience and mechanisms for rapid response to cross-border incidents are being established.

Judicial system of digital jurisdiction.

The state ensures the creation and functioning of digital courts, arbitrations and tribunals of a new generation that administer justice in a fully digital format. These institutions are empowered to handle disputes arising from digital transactions, blockchain transactions, digital asset transactions, Metaverse activities, DAOs, smart contracts, and other immersive environments where humans, avatars, or autonomous agents interact.

Decisions of digital courts are made collegially using algorithmic support for the analysis of evidence, but the final decision remains with the human judge. Such decisions are fully legally binding, digitally signed, automatically registered in the national register and can be executed through smart contracts within the digital jurisdiction of the State.

All disputes between subjects of digital law, regardless of their physical location, type of technology or method of communication, are subject to resolution in accordance with the norms of digital jurisdiction of the State, unless otherwise expressly provided for by international treaties or agreements on mutual recognition of jurisdictional procedures.

Digital jurisdiction covers both disputes between natural and legal persons, as well as between autonomous agents, digital avatars, robotic systems or hybrid artificial entities, if their activities create consequences in the national legal field. Such disputes may arise in the field of smart contract execution, distribution of digital assets, use of intelligent technologies, personal data protection, information security, cyber offences, violation of the terms of digital licences or algorithmic agreements.

Digital jurisdiction also applies to situations where the actions of artificial agents or algorithmic systems entail consequences for human rights, freedoms or duties — in particular, automated decision-making, management of digital property, or the creation of digital images of a person without consent.

Within the framework of digital jurisdiction, full procedural equality of the parties, regardless of their nature — human or digital — is ensured, with the right to representation, defence, appeal and enforcement of decisions in digital form.

The state creates and maintains an integrated digital ecosystem of digital justice, including a public register of electronic jurisdictional decisions, an electronic notary system, online testimony, digital arbitration, electronic certification of evidence, and mechanisms for instant enforcement of decisions through smart contracts.

The Public Register of Electronic Solutions is an open blockchain resource that guarantees the authenticity, immutability, and accessibility of solutions for all participants in the digital legal process. Each decision has a unique cryptographic identifier that allows you to verify its origin, time of adoption, and legal force.

The electronic notary system provides certification of actions, transactions and digital signatures in a fully electronic format, and online certification provides for the possibility of remote participation of parties, witnesses and experts in procedural actions in compliance with cybersecurity and authentication standards.

Mechanisms for instant enforcement of decisions through smart contracts ensure the automatic execution of judicial or arbitral acts in the digital environment without the need for additional administrative procedures. Notified bodies are obliged to guarantee full transparency of procedures, protection of personal and commercial data, as well as compliance of all decisions with the principles of fairness, openness, accountability and international compatibility.

5.4.7. Responsibility in Digital Jurisdiction.

Violation of the laws of digital jurisdiction, data manipulation, distortion of digital evidence, unauthorised interference with blockchain records, destruction or forgery of electronic documents, as well as refusal to enforce a digital court or arbitration award are grounds for legal liability.

Such violations include actions that undermine trust in digital justice systems, impede the execution of decisions, or create risks to national security in the digital space. They entail the application of measures in the form of blocking digital identifiers, temporarily restricting access to digital resources, cancelling registrations, revoking certificates of authenticity, imposing administrative sanctions, and in some cases, initiating criminal proceedings.

The state undertakes to establish mechanisms for monitoring, recording and investigating such offences using digital forensics, data audit systems and automated tools for tracking violations to ensure transparency and inevitability of responsibility.

At the same time, the State is developing a culture of legal thinking in the digital environment as a component of national identity and intellectual security. It provides training and advanced training of specialists in digital law, cyber law, digital ethics and information security, creates a new generation of educational programs for lawyers, judges, prosecutors, civil servants and technical specialists working in the field of digital governance.

The development of legal education within the digital jurisdiction includes the introduction of specialised courses, simulations of electronic trials, practice in digital laboratories of law, research of algorithmic decisions and modelling of court processes in the Metaverse.

An important direction is the formation of ethical codes for lawyers of the digital age, the development of legal research in the field of neural networks, autonomous systems and algorithmic judicial technologies that ensure justice, transparency and humanity in the application of e-justice.

5.5. The concept of the Metaverse Digital Code: theoretical and legal foundations

5.5.1. Key functional elements.

The exponential growth of digital flows, the emergence of non-classical legal entities — in particular, autonomous algorithms — and the intensive dynamics of innovations revealed the imperfection of the current regulatory mechanisms.

In response to these transformations, the concept of the Digital Code Model is proposed, a systemic regulatory document adapted to the needs of digital interaction within the paradigm of Society 5.0. Structurally, the model has a modular character, which ensures its flexibility, compatibility with international standards and the ability to evolutionarily adapt.

The key functional elements are: algorithmic updating of norms, automated legal monitoring using artificial intelligence technologies, as well as integrated mechanisms for ensuring a balance between technological progress, human rights and security needs of the state.

Special attention is paid to the architecture of the model and the strategy of its implementation, which provides for gradual integration into national and transnational legal systems. This approach allows us to create a stable, effective and future-proof basis of digital governance that is able to meet the requirements of the modern technological environment.

In the world legal opinion, the problem of forming an information code or a special law on information and regulation of the Internet is not new. It originates in the second half of the twentieth century — from the moment when the rapid development of telecommunications, and subsequently the emergence of the Internet, became catalysts for changing not only economic, but also legal systems. Among these were UNESCO recommendations on the information society (Aristova, 2009; UNESCO, 2024; World Summit on the Information Society, 2003), and the WSIS (World Summit on the Information Society) (n.d.) in the early 2000s.

In the scientific community, the ideas of the "information code" were actively discussed in Japan, France, Germany and the United States. For example, the French "Code de l'économie numérique" (Loi n° 2004-575, 2004)[1], which was partly a codification of norms in the field of digital commerce, electronic signature and data protection, became one of the first examples of a national approach to digital law. In Germany, the reform of the Bundesdatenschutzgesetz (Bundesdatenschutzgesetz, 2018)[2] — the Data Protection Act, which became the central legal mechanism for regulating information flows. In the United States, the model of the sectoral approach was more common, in which the main acts became the Communications Decency Act (47 U.S.C. § 230, n.d.)[3], Children's Online Privacy Protection Act (Federal Trade Commission, n.d.)[4], as well as a paternalistic interpretation of the First Amendment to the Constitution in the context of digital freedom of speech.

Modern digital laws of the European Union — in particular, the Digital Services Act (European Parliament & Council of the European Union, 2022)[5], Digital Markets Act, AI Act 2024 — constitute quasi-codes that already contain a modular structure and elements of platform self-regulation, algorithmic control, and data interoperability.

In the scientific plane, a thorough comparative legal study was carried out in the works of Lawrence Lessig "Code and Other Laws of Cyberspace" (Lessig, 1999), [6]who argued that the code and architecture of digital environments are already a de facto law, and the law should not only codify, but also form the ethical and infrastructural logic of digital systems. The idea of developing an integrated information code was actively promoted in Ukraine in the mid-2000s. However, the draft of this regulatory legal act turned out to be cumbersome and full of terminology, which is now outdated.

---

1 Law No. 2004-575 of June 21, 2004 on confidence in the digital economy. (2004). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/2021-07-26/

2 Federal Data Protection Act (BDSG). (2018). https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html.

3 47 U.S.C. § 230. (n.d.). *Protection for private blocking and screening of offensive material.* https://www.law.cornell.edu/uscode/text/47/230

4 Federal Trade Commission. (n.d.). *Children's Online Privacy Protection Act (COPPA).* https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-ac

5 European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act).* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

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

In the face of intense digital transformation, social and economic systems are undergoing profound structural shifts driven by the adoption of advanced technologies. In particular, artificial intelligence, cloud computing, quantum solutions, and immersive environments such as the Metaverse are shaping a new configuration of digital reality marked by high complexity, interactivity, and dynamics (Kostenko & Yekhanurov, 2024).[1]

In such conditions, traditional legal constructions — jurisdiction, legal personality, normative regulation — demonstrate significant limitations. Their effectiveness is decreasing against the backdrop of a globalised, decentralised, and fast-paced digital environment, to which classical legal instruments were not adapted. The current legal architecture, formed in the era of analog relations, is less and less in line with the parameters of modern technological realities.

5.5.2. Modular digital legal platform.

In response to these challenges, the Digital Code Model is proposed — a new generation regulatory system designed taking into account the peculiarities of the digital age. A distinctive feature of the model is its functional flexibility and ability to be constantly updated, which is achieved thanks to built-in algorithms of legal monitoring based on artificial intelligence and the activities of interdisciplinary expert bodies.

This combination of tools allows for the rapid adaptation of legal norms to changes in technological and social contexts. As a result, the model contributes to increasing the efficiency of legal regulation and ensures the proper compliance of the legal system with the conditions and risks of the digital environment. In this context, the Digital Code Model appears as a conceptually new paradigm of legal response to the challenges of the digital age. It is focused on ensuring a balance between the innovative development of technologies, the observance of fundamental human rights and the preservation of the institutional security of the state in the globalised information space.

The development of this model is a response to a number of fundamental problems facing modern jurisprudence in the era of digital transformation, in particular:

- Globalisation of digital flows. Unified digital transactions that cross state borders without physical presence make the traditional doctrine of territorial jurisdiction obsolete. This requires the introduction of new forms of transcontinental legal settlement and coordination mechanisms between national jurisdictions.
- The emergence of new legal subjects and objects. Digital agents built on the basis of artificial intelligence, as well as objects of the virtual economy (cryptocurrencies, NFTs, avatars, digital twins, etc.), do not have a clear regulatory status. The model of the Digital Code provides for the conceptual inclusion of these latest phenomena in the legal system with the definition of their legal personality, boundaries of legal responsibility and legal status within digital legal relations.
- Regulatory lag. Traditional law-making mechanisms based on hierarchical and procedurally burdened models of rule-making reveal inertia and inability

1 Kostenko, O., & Yekhanurov, Y. (Eds.). (2024). *Digital transformation in Ukraine: AI, metaverse, and society 5.0.* SciFormat Publishing Books. https://doi.org/10.69635/978-1-0690482-1-9.

to respond promptly to technological innovations. Such regulatory inertia complicates enforcement and creates situations of legal uncertainty.

- Fragmentation of the normative array. The lack of coherence between various sectoral and sectoral acts regulating digital relations leads to fragmentation of the legal space, the emergence of legal conflicts and a decrease in the effectiveness of legal influence. In response, the Digital Code Model provides an integrated architecture that ensures regulatory integrity and consistency.

The proposed Digital Code Model is built as a multi-level modular platform.

This approach allows not only to ensure the flexibility of legal response, but also to formalise mechanisms for dynamic updating of the regulatory framework. The architecture of the model covers a number of key components: algorithmic monitoring of legal changes, expert advisory mechanisms involving interdisciplinary expertise, as well as legal audit systems integrated with digital registers and open data infrastructure.

Particular attention is paid to the artificial intelligence module, which performs the function of the analytical core of the system. Its task is to constantly analyse the technological context, social transformations and changes in international law in order to promptly update regulatory provisions. The model provides for an open implementation roadmap based on the principles of gradual harmonisation with national legal systems and international standards.

Thus, the Digital Code Model serves as a conceptual foundation for building a new architectonics of digital law — adaptive, transparent and future-oriented. Its implementation will eliminate a number of key regulatory contradictions, ensure a high level of regulatory compliance with the challenges of the digital environment, and form effective digital governance as the basis for law and order in the post-industrial society.

5.5.3. Theoretical foundations of the digital code model.

The evolution of legal systems reflects the dynamics of social changes. In the industrial age, codes, specifically the Napoleonic Code, were created to regulate stable and localised social relations. At the same time, with the advent of the digital age, marked by the concept of Society 5.0, which provides for the harmonious integration of technology and human activity, there is a need for a new legal paradigm. Information law, as a branch in its own right, focuses on regulating digital interactions, data flows, and emerging legal entities such as AI agents and decentralised autonomous organisations (DAOs).

Digital transformation gives rise to a number of challenges, including the limitations of traditional concepts of territorial jurisdiction, the rapid pace of technological progress, and the fragmentation of the regulatory field. These factors emphasise the need to create adaptive legal systems that can evolve with technology, while maintaining the stability and predictability of legal regulation. The proposed Digital Code Model is also based on the principles of legal design, modular structure and semantic interoperability. It is aligned with international standards — in particular, the European Union Digital Acts (EUR-Lex) and the standards of the International Organization for Standardization (ISO) — ensuring global interoperability and efficiency.

The formation of the Digital Code Model involves the passage of several successive stages, each of which performs a specific methodological function:

- Doctrinal analysis of the regulatory framework. At this stage, a deep systematic study of the current array of legal acts in the field of information and digital law is carried out. The goal is to identify normative gaps, logical and semantic contradictions, as well as to identify norms that have lost their effectiveness in the conditions of new technological realities. Special attention is paid to institutional conflicts between sectoral regulations and supranational law.
- Comparative legal research. An analytical assessment of the leading models of digital regulation is carried out in order to extrapolate the most effective solutions. An important aspect is a critical understanding of the phenomenon of legal transplantation, which involves the adaptation of borrowed decisions, taking into account the local legal mentality and normative context.
- Legal design and machine-readable structure. This stage involves the engineering design of the model as a digital legal environment. Emphasis is focused on modularity, which ensures the construction of a system from separate logically complete components (legal domains, registration modules, access interfaces), as well as on machine-readability — the ability of legal norms to be interpreted by computer systems. This, in turn, provides automated interaction with other digital platforms (GovTech, LegalTech, FinTech).

The synthesis of these methodological approaches allows us to create not only an adaptive and scalable legal structure, but also to ensure its compliance with modern requirements for transparency, openness and functional interoperability. The application of this approach makes the Digital Code Model capable of continuous updating in accordance with changes in the sociotechnical environment, as well as integration into the international regulatory ecosystem due to compliance with ISO, W3C, IEEE standards and the UN institutional framework on digital rights and sustainable development.

As a result, the chosen methodology allows us to design a new generation of law — digital in nature, flexible in architecture, and value-oriented, which ensures not only regulatory efficiency, but also legal legitimacy in the age of the information society.

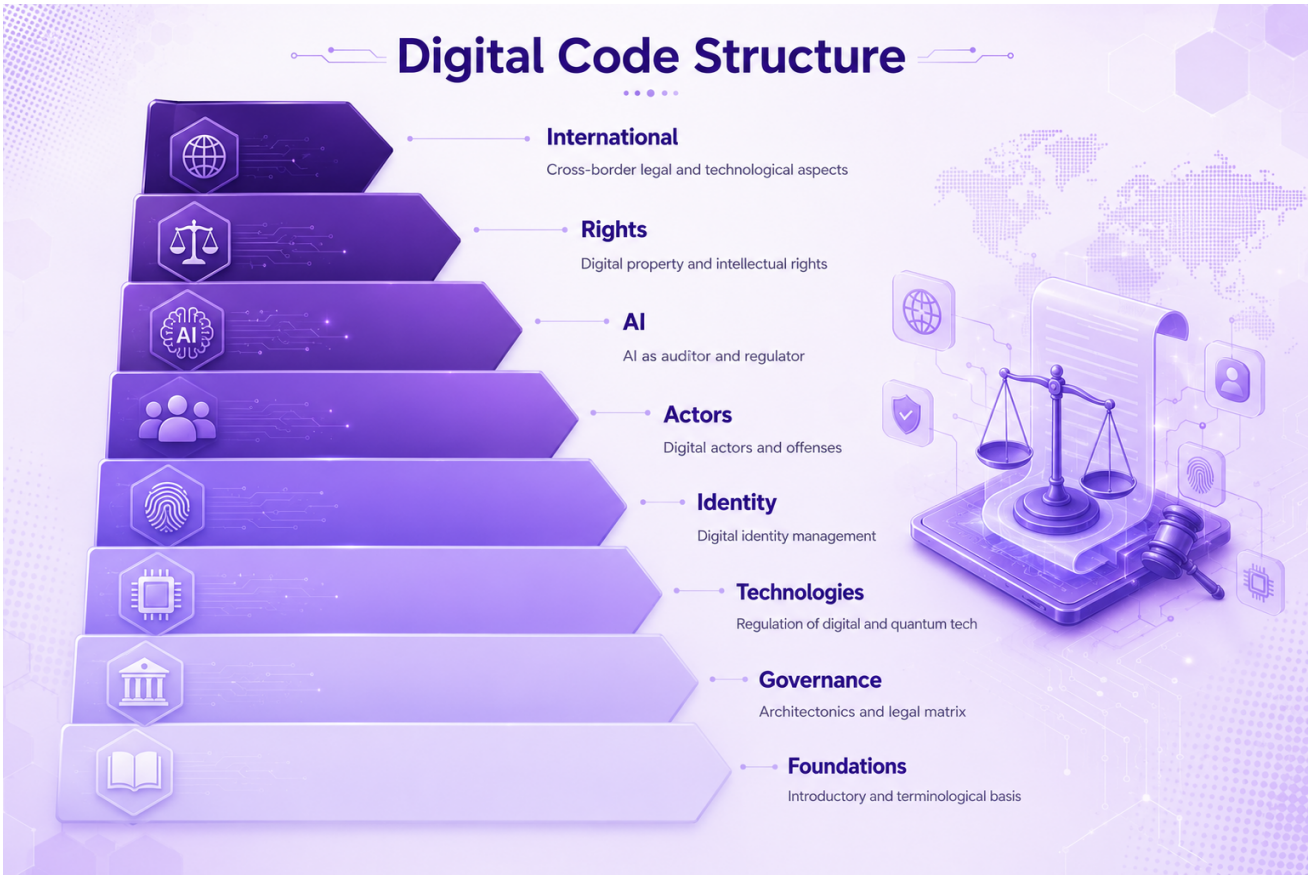


Figure 72. Digital Code Model Topology

The general topology of the Digital Code Model may consist of various modules that will structurally and systematically accommodate the regulatory functions of any sphere of human activity related to and created using modern information and immersion technologies (Figure 72).

Let's consider only the basic modules that will form the foundation of the Digital Code (Figure 73).

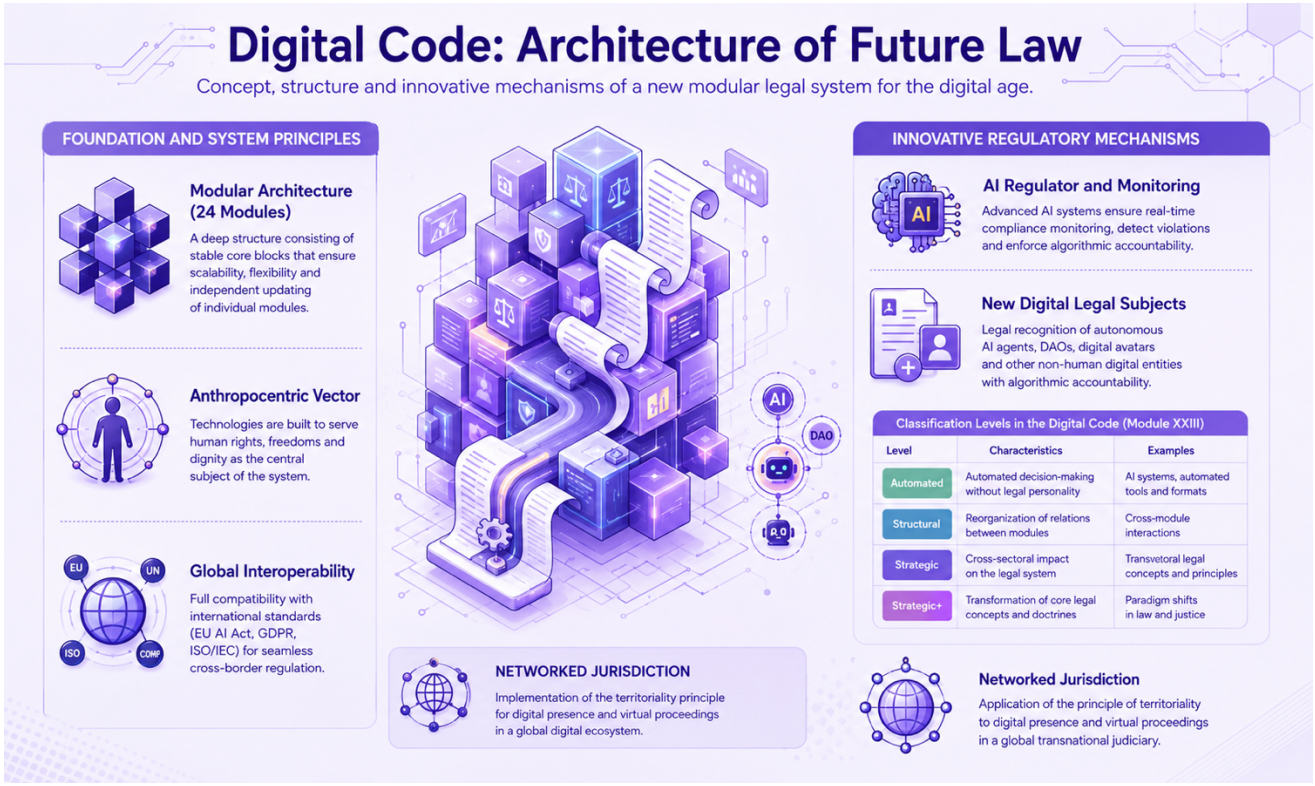


Figure 73. The Digital Code model is the architecture of the law of the future.

5.5.6. Digital Code Modules

Module I. Introductory part.

Module I forms the conceptual basis for the need to create a new legal system capable of meeting the challenges of the digital age. It justifies the limitations of traditional codes, which prove to be unable to cover new forms of legal relations arising from the action of autonomous agents, global digital flows, cryptocurrency assets, Metaverse interfaces, and virtual entities. The key problem is pointed out — the regulatory lag, which makes it impossible to timely respond to technological changes.

The proposed model provides for a modular structure that combines the stability of principles with the ability to quickly update. Its architecture is adapted to the integration of new legal categories and technological realities. The focus is on the idea of building a system that combines the stability of fundamental legal principles with the flexibility to adapt to dynamic changes. This format ensures the ability of law not only to react, but also to proactively shape the regulatory environment, including new categories of legal personality and forms of ownership.

The module also highlights the global dimension of digital processes and, accordingly, the need for inter-jurisdictional harmonisation. The need for harmonisation of legal regimes in the transnational digital environment is emphasised. The proposed model meets international standards and is designed taking into account the requirements of global interoperability.

It is envisaged to lay the foundations for transnational legal interoperability through the integration of international digital standards, such as the Digital Services Act, ISO/IEC, OECD Digital Governance Recommendations on Digital Governance, etc.

Thus, the Introductory Part serves as a theoretical and strategic foundation for the entire model, forming the starting positions for the formalisation of digital law in the context of technological turbulence and the era of post-industrial legal architecture.

Module II. Terminological and methodological basis.

The framework of the Module defines the semantic framework of the model by creating a dynamic, machine-readable and up-to-date glossary of digital legal terms. This glossary is not only a reference tool, but also an infrastructure element for the functioning of other modules, including norm repositories, digital solutions, smart contracts, and interoperable services.

Terminology is developed taking into account the principle of legal sovereignty in the definition of concepts, while ensuring consistency with international classifiers (e.g. EUR-Lex, WIPO Pearl, ISO/IEC 2382). The glossary functions as a "living dictionary" that is constantly updated by an interdisciplinary council of specialists — representatives of national jurisdictions and cross-border digital jurisdictions: lawyers, technoethicists, philologists and experts in information modelling.

Methodologically, the module is based on the concept of legal design and the principles of semantic interoperability. This allows for unambiguous interpretation of terms by both humans and machine intelligence, as well as integration with government and supranational digital governance systems.

As a result, Module II provides semantic integrity, logical consistency and technical adaptability of the entire array of legal norms of the Digital Code.

Module III. Fundamental provisions.

The Module formulates the basic principles of digital law, which are an integral part of the architecture of the Digital Code. They perform the function of a normative "axis" that guides the development of all subsequent regulatory provisions and practices. The key principles include: technological neutrality, digital inclusivity, respect for human rights, algorithmic responsibility, data security and transparency of algorithms.

These principles set moral and legal boundaries for digital governance, preventing technocentrism and normative relativism. Particular attention is paid to ensuring a balance between innovation and legal safeguards — for example, between automated decision-making and an individual's right to appeal (Bieliakov et al., 2023)[1].

The module also enshrines the priority of the human being as the central actor of the digital society: technologies should serve rights, freedoms and dignity, and not vice versa. Such an anthropocentric vector makes it possible to preserve the humanistic identity of law even within high-tech environments. At the same time, provisions are introduced that provide for the possibility of granting rights, duties and responsibilities to a certain class of digital subjects and objects.

Finally, the fundamental provisions serve as a methodological guide for the interpretation of all other provisions of the Digital Code and ensure the unity of the value approach in digital law-making.

1 Bieliakov, K. I., Tykhomyrov, O. O., Radovetska, L. V., & Kostenko, O. V. (2023). Digital rights in the human rights system. *InterEULawEast: Journal for the International and European Law, Economics and Market Integrations, 10*(1), 183–207. https://doi.org/10.22598/iele.2023.10.1.10.

Module IV. Repository of current regulations.

The creation of a centralised digital repository of relevant regulations governing digital processes is envisaged within the framework of Module IV. The repository performs the functions of saving, cataloguing, updating and automatically detecting outdated or conflicting norms. It is based on a semantic model of legislation, supported by means of artificial intelligence and machine analysis.

The repository allows you to integrate both national and international acts, ensuring their interoperability and adaptation to the local context. In addition, it supports the function of legal comparativeism — the ability to compare similar norms in different jurisdictions to harmonise digital regulation.

The process of updating the regulatory array is carried out both automatically (using update algorithms) and manually — by an audit conducted by an expert council. This approach ensures the constant relevance of legislation and the timely identification of regulatory gaps that require law-making response. The repository serves as the basis for the functioning of all digital regulation modules and acts as a guarantor of regulatory consistency.

Module V. Architectonics of Digital Governance.

This module defines the organisational and functional model of digital governance as a component of the institutional structure of the Digital Code Model. It is also planned to build a multi-level architecture, within which government agencies, digital regulators, scientific and expert councils, and AI modules of regulatory analysis interact.

The key element is the principle of symmetry between the human and machine components of governance. The system includes the use of digital interfaces for law-making, smart contracts in the field of administrative decisions, and digital platforms for real-time public consultations.

The module also includes provisions on management transparency, electronic document management, dynamic control and cross-sectoral coordination in the digital environment. Interaction with international governance institutions and regulatory compatibility with digital policies of the EU, OECD, ITU and other global structures is ensured.

The architectonics of digital governance outlined in the module creates the basis for an efficient, open and flexible regulatory environment that is in line with the principles of democracy, innovation and technological responsibility.

Module VI. Systemic and legal matrix of digital communication.

The regulatory framework for the functioning of digital communications infrastructure, in particular Internet protocols, telecommunications platforms, satellite communications, data exchange systems and next-generation (5G/NG) architectures, is set out in Module VI. The module ensures the integrity of the legal regulation of information exchange in the context of decentralised and cross-border networks.

The main areas of regulation include: spectrum management, technical standards and interfaces, licensing of operators, protection of user rights, protection of critical information infrastructure and ensuring non-discriminatory access to digital communications.

The module provides for the introduction of dynamic regulatory monitoring based on AI, which allows detecting violations or failures in the legal regime of

telecommunications. In addition, it is envisaged to create a mechanism for digital attribution of responsibility between providers, platforms and end users.

The legal matrix of communication is a key tool for ensuring the sustainability of digital sovereignty, national security and protection of rights in the virtual public sphere. It forms the basis for interaction between users, the state and transnational operators of digital services.

Module VII. Digital jurisdiction.

The Module develops the legal doctrine of jurisdiction in the digital space, taking into account new forms of cross-border interaction, the absence of physical localisation of servers and the specifics of the activities of digital environment subjects. It moves away from classical territorial approaches, proposing functional, network, and algorithmic jurisdictional models.

The concepts of digital presence, data storage locations, transaction coding (code of actions) and verification of participants using cryptographic methods are introduced. The criteria for jurisdictional binding in smart contract systems, decentralised platforms, Metaverse environments, and blockchain infrastructures are determined.

The module also regulates the procedure for recognising electronic evidence, digital transactions, and the responsibility of participants in a multi-jurisdictional environment. Mechanisms for mutual delegation of jurisdiction between national systems and the creation of supranational digital arbitration are provided.

Digital jurisdiction acts as a key tool for providing legal certainty in transnational digital processes, allowing to establish a connection between the subject, the digital environment and the applicable law in a complex information landscape.

Module VIII. Legal regulation of digital technologies

The module establishes a regulatory framework for the development, implementation, and control of the use of modern digital technologies — artificial intelligence, the Internet of Things (IoT), blockchain systems, neural networks, big data (Big Data), cloud platforms, and automated interfaces.

The central task is to ensure a balance between stimulating innovation and preventive legal control. Requirements are introduced for the transparency of algorithms, the explainability of decisions made, a risk-oriented approach to the classification of technologies, as well as the principle of responsibility of the developer and operator.

Special attention is paid to the observance of ethical standards and human rights in automation processes, in particular non-discrimination, protection of privacy and the right to refuse machine intervention. Mechanisms for certification of digital systems, licensing of critical technologies and regulatory modelling of pilot projects are provided.

The module is based on the principles of technoethical legitimacy, dynamic legal support of the innovation cycle, and integration with global digital regulatory initiatives, including the EU AI Act, IEEE Ethically Aligned Design, as well as UNESCO recommendations on AI ethics.

Module IX. Legal regulation of quantum technologies

This module defines the legal framework for the use, development and circulation of quantum technologies as critical elements of the future digital infrastructure. The focus is on quantum computing, quantum cryptography, quantum communications, and quantum sensors.

Legal regulation provides for the introduction of post-quantum security standards, the development of audit and certification mechanisms for quantum products, as well as the creation of a special legal regime for quantum research platforms. The concept of a "quantum trace" — a digital token of actions in a quantum environment, which is the basis for legal attribution, is introduced.

The module pays special attention to international cooperation in the field of quantum governance, ethical constraints on the development of destructive or opaque quantum systems, and the role of the state in ensuring technological sovereignty through the creation of quantum hubs.

In the legal plane, the module establishes an interface between classical norms of digital law and the new quantum legal regime, proposing mechanisms for joint action, updating the regulatory framework, and proactive monitoring of risks associated with the hypercomputing power of future quantum machines.

Module X. Digital Identity Management

The module establishes the regulatory framework for the functioning of digital identification systems in a virtualised legal environment. It covers the legal regulation of personal identifiers (digital profile, biometric and behavioural markers), authentication, verification and access control mechanisms (Kostenko & Mangora, 2022e).[1]

The concept of digital identity as a multi-level legal construct that includes decentralised elements, blockchain records, zero-knowledge proofs, and digital subscriptions is being introduced. The principles of data minimisation, user control, voluntary consent and the right to be forgotten are established.

The module defines the requirements for digital identity service providers, introduces trust categories (trusted level, critical level, limited level), and also contains mechanisms for liability for compromise or unauthorised use of identification systems.

Thus, the module creates a legal basis for the formation of a secure, ethically sound and technically interoperable digital identity infrastructure in the context of global data exchange and interaction of jurisdictions.

Module XI. Legal regulation of immersion technologies

The module focuses on the regulatory support of the development of immersion technologies — virtual (VR), augmented (AR), and mixed reality (MR), etc. It defines the legal framework for the use of immersive platforms in the fields of education, healthcare, public administration, entertainment, and e-commerce.

Within the module, the criteria for digital presence, the legal status of the immersive user, as well as the rules for the functioning of virtual environments with a high level of immersion are established. The concept of "virtual legal personality" is introduced and the status of virtual avatars as carriers of actions in the digital space is regulated.

Legal regulation also covers aspects of mental impact, cyber-physical consequences and content liability. Standards for the safe use of VR/AR devices, restrictions for vulnerable categories of persons, ethical standards of immersion, and rules of digital behaviour in an immersive environment are defined.

1 Kostenko, O. V., & Mangora, V. V. (2022e). Directions of legal regulation development of identity data management. *Information and Law, 1*(40), 54–60. https://doi.org/10.37750/2616-6798.2022.1(40).254342

Module XI is key to shaping the concept of "virtual ethics", protecting personal data in deeply interactive environments, and developing legislation that regulates the "new reality" that combines physical, digital and emotional-cognitive dimensions.

Module XII. Legal regulation of the Metaverse

Module XII establishes a regulatory model for regulating the Metaverse as interactive virtual environments operating on the basis of immersive technologies, blockchain infrastructures, and artificial intelligence algorithms. The goal is to form a legal framework for activities in decentralised virtual spaces (Kostenko & Holovko, 2023b).[1]

The concepts of digital territoriality, tokenised jurisdiction, virtual citizenship, and contractual reality are being introduced. Legal regimes for transactions in Metaverse ecosystems are defined, including the circulation of NFTs, digital assets, virtual land plots, and avatar representations.

The module establishes standards for authenticating actions, fixing transactions, resolving conflicts, and moderating content. Mechanisms for self-regulation of virtual communities, transparency of interaction protocols, and legal responsibility in cases of cybercrime or violations of digital identity ethics are provided (Kostenko, 2022f).[2]

Thus, Module XII creates conditions for the development of the participatory economy, digital self-government, and transnational inclusion in Metaverse platforms, integrating the tools of ethical governance, digital democracy, and the normative balance between the virtual and real legal worlds.

Module XIII. Digital Actors

The module identifies new types of legal entities arising from the functioning of digital environments, including artificial agents, digital avatars (Kostenko & Mangora, 2022d), [3]autonomous organisations (DAOs), robotic systems, and virtual representative offices. Its goal is to formalise the participation of these actors in legal relations.

The concept of algorithmic legal capacity is introduced, reflecting the ability of AI systems to initiate, change or terminate legal consequences within certain scenarios. The module establishes criteria for limited and conditional legal personality, regulates delegation of authority and algorithmic responsibility.

The focus is on creating registers of digital entities, determining their role in transactions, as well as mechanisms for control, supervision and revocation of delegated powers. Particular attention is paid to balancing between the autonomy of digital subjects and human supervisory functions (human preservation).

Thus, the module forms a legal basis for the inclusion of non-classical participants in the system of public and private law, defining the boundaries of their participation, responsibility and legitimacy in the digital legal order.

---

1 Kostenko, O. V., & Holovko, O. M. (2023). Electronic jurisdiction of the metaverse: Challenges and risks of legal regulation of virtual reality. *Information and Law, 1*(44), 105–115. http://ippi.org.ua/kostenko-ov-golovko-om-elektronna-yurisdiktsiya-metaverse-viklik-ta-riziki-pravovogo-regulyuvannya

2 Kostenko, O. V. (2022f). Artificial intelligence (AI) and the metaverse: Legal aspects. *Juridical Scientific and Electronic Journal, 8*, 301–308. https://doi.org/10.32782/2524-0374/2022-8/66.

3 Kostenko, O. V., & Mangora, V. V. (2022). Metaverse: Legal prospects for regulating the use of avatars and artificial intelligence. *Legal Scientific Electronic Journal, (2*), 102–105. https://doi.org/10.32782/2524-0374/2022-2/23

Module XIV. Digital offences and punishments

The module systematises the categories of offences specific to the digital environment and establishes mechanisms for bringing to legal responsibility in the field of information legal relations. Module XIV covers both traditional forms of cybercrime (unauthorised access, malware, data manipulation) and the latest violations related to autonomous systems, algorithms, and virtual environments (Kostenko et al., 2023a)[1].

The concepts of algorithmic guilt, digital intent, and machine negligence are introduced. A matrix of punishments is formed, taking into account both the legal nature of the subject (human, AI, DAO) and the level of risk, the degree of public danger, and the level of autonomy of actions (Casino et al., 2022)[2].

Particular attention is paid to the regulation of digital evidence, attribution of offences, jurisdictional cooperation, as well as the implementation of the principle of digital justice. The functions of digital prosecutors' offices, virtual courts and monitoring centres for digital behaviour are defined.

The module provides a regulatory response to the growing number of threats in cyberspace, increases the effectiveness of prevention, contributes to the restoration of justice and lays the foundations for a new generation of global digital criminal policy.

Module XV. Artificial intelligence as a digital monitor-auditor

Module XV establishes the functional role of artificial intelligence in the digital law system as a tool for continuous analytical monitoring (Leocádio et al., 2024)[3], revision and interpretation of the normative array (Meitasari & Audrey, 2023)[4]. AI is considered as an autonomous auxiliary link in identifying legal conflicts, irrelevant norms, as well as contradictions between digital practices and current legislation.

A model of algorithmic analysis of legal acts, integrated with the repository of current norms, is introduced (Hanfy et al., 2024)[5]. AI carries out thematic structuring, time verification, classification by relevance, and risk analysis of possible regulatory gaps (Rao, 2024)[6].

The results of AI monitoring are presented in the form of reports, analytical dashboards, and recommendations for law-making and control bodies. There is a restriction on the autonomous intervention of AI in law enforcement — it is allowed only accompanied by a human curator.

As a result, the module forms the normative architecture of built-in digital self-control, ensuring the stability, relevance and accountability of the legal system in a highly dynamic digital environment.

---

1 Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). Metaverse: Model criminal code. *Baltic Journal of Economic Studies, 9(4),* 134–147. https://doi.org/10.30525/2256-0742/2023-9-4-134-147

2 Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). *SoK:* Cross-border criminal investigations and digital evidence. arXiv. https://doi.org/10.48550/arXiv.2205.12911

3 Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial intelligence in auditing: A conceptual framework for auditing practices. *Administrative Sciences, 14*(10), 238. https://doi.org/10.3390/admsci14100238.

4 Meitasari, R., & Audrey, A. (2023). Artificial intelligence in the big data era and digital audit. *Initiative: Journal of Economics, Accounting and Management, 2*(2), 91–104. https://doi.org/10.30640/inisiatif.v2i2.714.

5 Hanfy, F., Alakkas, A., & Alhumoudi, H. (2024). Analyzing the role of digitalization and its impact on auditing. *Multimedia Tools and Applications*, *83*(15), 1–22. https://doi.org/10.1007/s11042-024-19729-0.

6 Rao, N. (2024). Audit through artificial intelligence tools. *The Management Accountant Journal, 59*(10), 61–62. https://doi.org/10.33516/maj.v59i10.61-62p

Module XVI. AI Regulator in the Digital Code System

The module outlines the architecture and powers of the digital AI regulator as a permanent institutional component of the Digital Code system. Its function is to coordinate, examine, update and adapt the regulatory environment based on the recommendations generated by artificial intelligence.

The structure of the module provides for interaction between the AI regulator, the National Expert Council (NER) and the Main Scientific and Expert Environment. AI performs primary analytics, forms project proposals for changes to legislation, and simulates scenarios of legal impact.

The regulator acts within the conditions of normatively defined boundaries and according to clearly prescribed procedures: all recommendations are filtered through human commissions, verified for compliance with the values of the legal system, and published for public discussion.

As a result, the AI regulator ensures the dynamic stability of the digital regulatory system, forming a reasonable environment for law-making — analytical, predictable, evidence-based, and controlled.

Module XVII. Digital Property Rights and Intellectual Property

The module defines the regulatory framework for the legal regime of digital property and objects of intellectual activity in the virtual environment. It covers tokenised assets (NFTs), digital works, artificially generated content, software, data, algorithms, and digital things, etc. (Foster, 2023)[1].

The concept of "digital thing" as an independent object of civil circulation, which is subject to the legal regime of ownership, use and disposal, is introduced. The methods of confirming ownership through blockchain registers, digital signatures, cryptographic protocols and quantum tokens are determined (Zeynalov, 2021)[2].

In the field of intellectual property, the module regulates the creation, licensing, transfer, and protection of rights to AI-generated objects (Baiurchak & Kiriiak, 2024)[3]. A new category of authorship is proposed — "algorithmic (digital) author" — with a delegated legal status. Collective authorship in DAOs and Smart-IP agreements is also regulated.

The module creates prerequisites for a transparent, fair and technologically adaptive ownership system in the digital economy, contributing to the development of creative industries, cyberfinance and inter-jurisdictional integration in the field of digital asset circulation.

1 Foster, C. (2023). Intellectual property rights and control in the digital economy: Examining the expansion of M-Pesa. *The Information Society, 40*(1), 1–17. https://doi.org/10.1080/01972243.2023.2259895

2 Zeynalov, N. (2021). The issue of intellectual property rights in the digital world. *ANCIENT LAND: International Scientific Journal on Humanities and Social Sciences, 3*(2), 49–51. https://doi.org/10.36719/2706-6185/04/49-51.

3 Baiurchak, M., & Kiriiak, O. (2024). Intellectual property rights within the digitization. In *Digitalization of legal deeds in the context of the modernization of public services* (pp. 93–98). https://doi.org/10.59295/daj2022.13.

Module XVIII. Cyber diplomacy

The module develops the conceptual and normative foundations of cyber diplomacy as a tool of state foreign policy in the digital environment. Cyber diplomacy (Banihashemi, 2021)[1] is considered as a system of multi-level legal and technopolitical measures aimed at resolving cross-border incidents, coordinating international law-making and ensuring digital sovereignty (Tsagourias, 2018; Dragomir, 2021)[2,3].

The module provides for the creation of cyber missions in UN, EU, ITU, national jurisdictions, as well as the development of digital diplomatic protocols to resolve incidents related to cyberattacks, data breaches, platform blocking, or regulatory conflicts (Kostenko et al., 2024b) (Mutimer, 2004)[4].

It is planned to create a state hub "Cyber Tribune", which provides technical support, legal position and analytics for international negotiations in the field of digital technologies. The status of a cyber diplomat, the procedure for accreditation, the list of powers and the rules of ethical behaviour in digital interactions are defined.

As a result, the module forms a new branch of public international law — digital diplomacy — as a reaction to the transformation of geopolitical interaction in the era of deep digitalisation.

Module XIX. Cross-border legal and technological sandbox

The module defines the regulatory framework for the creation of cross-border legal and technological sandboxes — special regulatory regimes for testing innovative digital solutions in a legal environment adapted to rapid technological changes (Kostenko et al., 2024c)[5].

The sandbox functions as a limited digital environment with modified norms (Truby et al., 2022)[6], within which actors can implement experimental products: AI platforms, blockchain infrastructures, quantum services, digital currencies, virtual jurisdictions, SmartLaw protocols (Tsai et al., 2020)[7].

Mechanisms for preliminary risk assessment, temporary authorisation, supervisory examination, and conditional liability are being introduced (Beckstedde et al., 2023)[8]. Sandbox participants operate under the control of a digital supervisory board and have the obligation to publicly report on the results of the experiment.

---

1 Banihashemi, S. S. A. (2021). *Cyber diplomacy*. https://doi.org/10.9734/bpi/mono/978-93-91473-74-7.

2 Tsagourias, N. (2018, July 13). *Law, borders and the territorialisation of cyberspace*. SSRN. https://doi.org/10.2139/ssrn.3213511.

3 Dragomir, A. (2021). Cyber diplomacy. *International Journal of Information Security and Cybercrime, 10*(2), 37–50. https://doi.org/10.19107/ijisc.2021.02.05.

4 Mutimer, D. (2004). Cyber-diplomacy: Managing foreign policy in the twenty-first century. *Canadian Journal of Political Science, 37*(4), 1066–1068. https://doi.org/10.1017/S0008423904480214.

5 Kostenko, O. V., Volkova, Y. A., Ustynova, I. P., Shapenko, L. O., & Usenko, Y. V. (2024c). Legal perspectives of the international scientific sandbox metaverse: Technologies and foresights for digital transformation. In *Advanced metaverse wireless communication systems* (Chap. 18, pp. 519–548). https://doi.org/10.1049/PBTE112E_ch18.

6 Truby, J., Dahdal, A., & Ibrahim, I. (2022). Sandboxes in the desert: Is a cross-border "gulf box" feasible? *Law, Innovation and Technology, 14*(2), 447–473. https://doi.org/10.1080/17579961.2022.2113674.

7 Tsai, C. H., Lin, C. F., & Liu, H. W. (2020). The diffusion of the sandbox approach to disruptive innovation and its limitations. *Cornell International Law Journal, 53*(2), 1–37. http://dx.doi.org/10.2139/ssrn.3487175.

8 Beckstedde, E., Ramírez, M., Cossent, R., Vanschoenwinkel, J., & Meeus, L. (2023). Regulatory sandboxes: Do they speed up innovation in energy? *Energy Policy, 180*, 113656. https://doi.org/10.1016/j.enpol.2023.11365.

Thus, the Module allows the legal system to adapt to the latest technologies in the "controlled flexibility" mode, ensuring a balance between security, innovation and integration into the international techno-legal space.

Module XX. Cross-Border Digital Court

Module XX describes the legal architecture of establishing a cross-border digital court as a dispute resolution tool in a multi-jurisdictional digital environment (Mańko et al., 2022; Onţanu, 2019)[1,2].

The court operates on the basis of cloud infrastructure, smart contracts, and virtual presence technologies.

The court will specialise in the following areas: disputes over blockchain transactions, digital assets, violations in the Metaverse, actions of AI systems, algorithmic fraud. The principles of procedural neutrality, digital evidence, virtual confidentiality and automated enforcement of decisions are being introduced.

Court hearings take place in virtual rooms with the provision of participant authentication, data protection and visual representation of legal actions. There is an adaptive interface module for judges, parties and the public, as well as the ability to integrate with external digital jurisdictions.

As a result, the cross-border digital court appears as an innovative judicial platform that ensures speed, accessibility and fairness in the consideration of digital disputes at the global level.

Module XXI. International Legal Inspection Office

This Module defines the status, powers and institutional model of the International Legal Audit Office — a supranational body for monitoring compliance with digital legal standards in a cross-border environment.

The International Office performs the functions of independent assessment of the legal climate of the Member States, verification of compliance with digital integrity standards, publication of analytical reports on the effectiveness of regulatory policies, and detection of digital anomalies (Yang et al., 2023)[3].

The office's toolkit includes: expert audits of digital policies, real-time analysis of regulatory data, conducting cloud inspections, providing advice for governments and developers (Zhu et al., 2024).[4] The activities are coordinated with the structures of the UN, the EU, the Council of Europe, WIPO, ISO (Burk, 2005)[5].

The module aims to increase the transparency of digital governance, form a global mechanism of regulatory responsibility and support the sustainable development of the digital space in the interests of humanity.

---

1 Mańko, R., Epp, P., & Radev, E. (2022). Computerised system for communication in cross-border judicial proceedings (e-CODEX). *Computer Science, Law*. https://api.semanticscholar.org/CorpusID:253519392.

2 Onţanu, E. (2019). Adapting justice to technology and technology to justice: A coevolution process to e-justice in cross-border litigation. *European Quarterly of Political Attitudes and Mentalities, 8*(2), 54–74

3 Yang, Y., Chen, N., & Chen, H. (2023). The digital platform, enterprise digital transformation, and enterprise performance of cross-border e-commerce: From the perspective of digital transformation and data elements. *Journal of Theoretical and Applied Electronic Commerce Research, 18*(2), 777–794. https://doi.org/10.3390/jtaer18020040.

4 Zhu, L., Yang, L., Li, C., Hu, S., Liu, L., & Yin, B. (2024). LegiLM: A fine-tuned legal language model for data compliance. *arXiv*. https://doi.org/10.48550/arXiv.2409.13721

5 Burk, D. L. (2005). Legal and technical standards in digital rights management technology. *Fordham Law Review, 74*(2), 537–573. https://doi.org/10.2139/ssrn.699384

Module XXII. International Scientific Expert Council on Digital Technologies, Ethics and Law

Module XXII defines the regulatory and organisational framework for the establishment of the International Scientific Expert Council, a multinational interdisciplinary body that provides ethical, legal, and technological expertise of digital transformations.

The Council is formed from leading scientists, digital ethicists, technology lawyers, developers, and analysts from different countries (Mahieu et al., 2018).[1] The main functions are: preparation of international standards of digital behaviour, assessment of legal risks of the latest technologies, advising international organisations and states on the observance of human rights in the digital sphere (Rochel, 2023).[2]

The module also provides for the development of a Code of Ethics for Digital Civilisation, the Council's participation in the implementation of global initiatives on responsible AI, digital security ecosystems, eco-digital balance, as well as the formation of academic platforms for legal foresight.

Thus, the International Council is becoming a key analytical-prognostic and normative-ethical actor that ensures a civilisational balance between technological progress and fundamental human rights in the era of digital evolution.

Module XXIII. Algorithmics of amendments to the Digital Code

Module XXIII defines the principles, structure and procedures for amending the Digital Code (hereinafter referred to as the Code). Its goal is to ensure the adaptability, stability and technological compatibility of the regulatory system in a fast-paced digital environment. A multi-level system of modifications is being introduced: algorithmic, structural, tactical and strategic changes.

Algorithmic changes provide for the automatic updating of wordings of norms, terminology, and interoperability formats through integrated AI monitoring — without affecting the content core of the Code (Sattlegger, 2024)[3]. Structural changes include the reorganisation of modules, their interconnections, and the creation of new submodules. Tactical changes concern the updating of specific norms, while strategic changes are aimed at transforming the general concept and paradigm of the Code.

The procedure for changes is based on an automated system for processing initiatives, which includes:

1) AI-monitoring of the regulatory environment;
2) semantic classification of changes (according to criteria G1-G5);
3) formalisation of proposals in the SmartNorm Draft format;
4) digital expertise by an AI regulator;
5) verification by the National Expert Council;
6) public discussion;
7) official approval (automatic or parliamentary).

---

1 Mahieu, R., Van Eck, N. J., Van Putten, D., & Van den Hoven, J. (2018). From dignity to security protocols: A scientometric analysis of digital ethics. *Ethics and Information Technology, 20*(3), 175–187. https://doi.org/10.1007/s10676-018-9457-5.

2 Rochel, J. (2023). Error 404: Looking for trust in international law on digital technologies. *Law, Innovation and Technology, 15*(1), 148–184. https://doi.org/10.1080/17579961.2023.2184139.

3 Sattlegger, A. (2024). Ethical governance of emerging digital technologies in the public sector: Insights from Dutch digital ethics commissions. In *Public governance and digital transformation* (pp. 131–146). https://doi.org/10.1007/978-3-031-70804-6_9

For critical situations, an accelerated procedure for changes is provided: AI generation of the project, dashboard publication, temporary provision, parallel verification. The fundamental provisions of Modules I–III are subject only to strategic changes under a special order.

The module enshrines the following principles: transparency (change register, public versions), accountability (analytical justification), stability (kernel preservation), and interoperability. Thus, the Digital Code acquires the properties of a self-educational, controlled and normatively stable digital system.

Module XXIV. Transitional and final provisions

Module XXIV consolidates the legal framework for the implementation, approbation and integration of the Digital Code Model into national legal systems, as well as defines mechanisms for its gradual adaptation to the global regulatory space.

It is determined that from the moment of entry into force, the basic modules of the Digital Code — Modules I-XXIII — have a direct regulatory effect and are subject to mandatory inclusion in national legal systems without changes. Their status is unified for all states participating in digital jurisdiction and serves as a universal legal foundation for the digital order.

Other modules can be implemented in stages through legal mechanisms determined by the domestic legislation of each state, taking into account national priorities, the level of digital transformation and participation in international digital institutions.

In case of amendments or additions to the provisions of any of the modules of the Digital Code, due to the emergence of new cross-border relations, breakthrough digital technologies or updating of ethical standards, such changes are automatically applied in all national jurisdictions that have ratified the Code. Their application is carried out in a holistic, authentic format, without modifications, and is considered part of the national legislation in accordance with the principle of digital integrativity.

It is envisaged to create an International Synchronisation Platform (Digital NormSync Hub), which provides simultaneous updates, verification and publication of current versions of the Model in all national digital registers.

At the transitional stage of implementation, the provisions of the Model are subject to testing within the framework of special modes of digital experiment — legal sandboxes (Regulatory Sandboxes), digital districts (SDZ), or educational platforms based on higher education institutions and technological development centres.

The module defines the principle of stability of fundamental norms, transparency of changes, publicity of procedures, and also confirms mandatory compliance with international standards.

Thus, Module XXIV guarantees the integrity and legal effectiveness of the Digital Code in the context of global legal evolution and forms the infrastructure for its sustainable international functioning.

The presented Digital Code Model not only meets this challenge, but also lays the architectonics of a new legal dimension based on the principles of dynamism, interoperability, machine readability and ethical and legal responsibility.

The structure of the Code, organised according to the modular principle, allows you to synchronise the need for stability of the legal field with flexibility in terms of technological breakthroughs. Each module functions as an autonomous but integrated

unit of normative action, ensuring the scalability of the system, its expansion and adaptation to the international context. This approach meets not only the logic of digital governance, but also the legal needs of the knowledge society, in which a significant part of social interaction is mediated by algorithms.

Especially important is the idea of algorithmic updating of legal norms embedded in the Model — in combination with human expertise, public participation and an international verification mechanism. This creates a new format of legal legitimation, which takes into account speed, transparency and responsibility at the same time. The introduced system of digital auditor, ethics councils and international control guarantees a high level of quality and relevance of legal content.

The institutional vision set out in the Model allows for the gradual implementation of its provisions in national legislation, creating the basis for global legal unification without losing sovereignty. At the same time, it remains open to legal pluralism and local initiatives that do not contradict the principles of digital integrity. The interaction between automatic mechanisms and normative creativity of a person determines the face of the post-industrial legal order.

Thus, the Digital Code Model is not only a normative document, but also a conceptual manifesto of a new era of legal civilisation. It paves the way for digital sovereignty, technological justice, and global legal balance in a world where law not only regulates, but also shapes digital reality.

5.6. Theoretical and Legal Model of the Digital Criminal Code for the Metaverse.

The current stage of development of law is characterised by the fact that in the age of information, criminal law gradually gives its role to various specialised laws. Of course, the role of Criminal Codes does not decrease due to the delegation of criminal law norms to other areas of special law, but this trend is not quite optimistic. This was effective in the times of the scientific and technological revolution 4.0 and Web 2.0. Together with the development of information and communication technologies and Web 3.0 technologies, it became obvious that the dispersion of criminal law norms creates a legal dysfunction that does not contribute to the qualitative legal regulation of modern social relations. The Metaverse Model Criminal Code should concentrate the maximum necessary legal norms for regulating relations in virtual environments, and it is not identified exclusively with cybercrime laws (Lee, 2022)[1] and does not duplicate traditional Criminal Codes. The Metaverse Model Digital Criminal Code should become composite and combine many components with significantly different properties, which, when combined, will lead to the emergence of a new area of legal regulation relationships that are impossible in the analog world. In addition, the Metaverse Model Digital Penal

1 Lee, W. S. (2022). The role of criminal law in the metaverse. *Chonnam National University Law Review, 42*(3), 177–202. https://doi.org/10.38133/cnulawreview.2022.42.3.177

Code will explore the emergence of new torts in the virtual world and their consequences for the subjects and objects of the inhabitants of the virtual world and legal landscape.

Today, it is difficult to predict the entire range of socially dangerous acts and damage that can be committed in the Metaverse, as well as what misdeeds of a person, human prototype, avatar, electronic personality, electronic subjects and objects will have signs of a criminal offence in the future.

There is no understanding of what types of punishments or state coercion should be applied to socially dangerous acts of a person, a prototype person, an avatar, an electronic personality, electronic subjects, and objects in the Metaverse.

Thus, the Metaverse Model Digital Criminal Code may consist of several fundamental parts, which, in turn, will consist of relevant sections and articles (Figure 74):

Part 1 – Glossary or list of technical, technical-legal, legal concepts, norms and terms applied in the Metaverse and in related, specific areas of law.

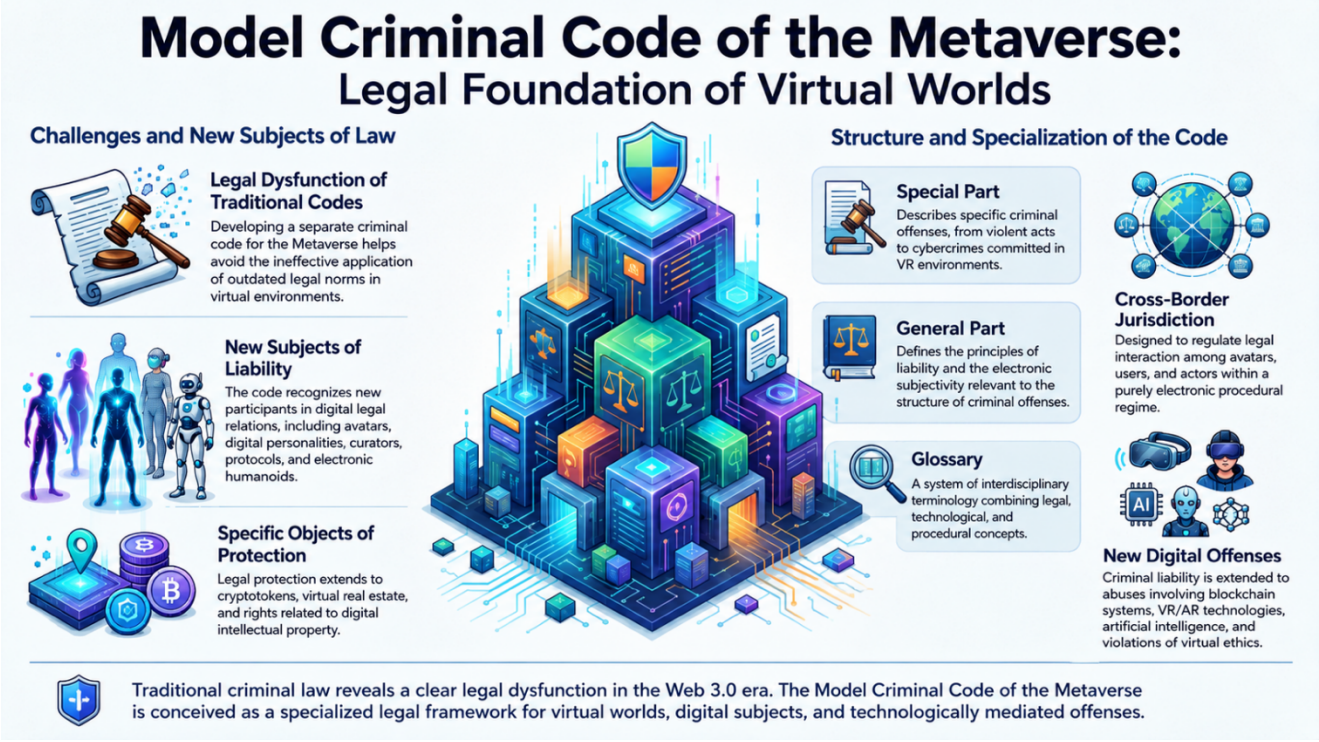


Figure 74. Model Digital Penal Code Metaverse

Part 2 – Metaverse cross-border regime law defines the mechanisms for establishing jurisdictions of various types, interaction between analog jurisdictions, between analog and electronic jurisdictions, between electronic jurisdictions.

Part 3 – The General Part of the Metaverse Digital Criminal Code defines the types and stages of crimes in the analog, mixed and virtual worlds, subjects and objects of crime, guilt and its forms, complicity in crime, punishment and its types, exemption from criminal liability, imposition of punishment, criminal record, repetition of crime, features of criminal liability of electronic subjects, avatars, electronic humanoids, etc.

Part 4 – The norms and torts of analog, mixed and electronic jurisdictions determine the types of socially dangerous acts or crimes, as well as criminal penalties that will be applied to persons, subjects, avatars, electronic humanoids.

Part 5 – Transitional provisions contain interpretations and procedural algorithms for making additions, amendments, application of archaic, national, cross-border norms of law, etc.

Part 1 is intended to form a conceptual and categorical apparatus used in the fields of law related to the Metaverse. Obviously, the vast majority of terminology is of a technical nature and content that do not correlate with legal norms. It is advisable to form an interdisciplinary conceptual and categorical apparatus, which will become a single base of norms and definitions, which will simplify the formation of standard normative legal acts for their simultaneous use in different jurisdictions, and will encourage national legislation to revise legislation.

Part 2 aims to form the main mechanisms for determining or establishing the regime of cross-border interaction between information and communication systems and virtual spaces of different territories and jurisdictions. First of all, such mechanisms or algorithms should provide a simple and reliable identification and classification of events in electronic environments, which will allow them to be divided into ranks by territories, physical and electronic jurisdictions. Such an approach will not only simplify the definition of jurisdictions, but will also contribute to the transformation of national judicial systems by creating appropriate judicial institutions to operate in the Metaverse.

Part 3 of the general digital part of the Metaverse Criminal Code should contain norms that establish the principles and general provisions of criminal law, the validity of criminal law in space and time, defines the concept of crime, stages of committing an intentional crime, signs of the subject of the crime, the content of guilt, the concept of complicity, types of multiple crimes, circumstances that exclude the criminality of the act, the grounds for exemption from criminal liability and from punishment and its serving, general principles of imposing punishment, etc.

Part 4 consists of parts (sections that unite a certain group of descriptions of crimes located in it, similar to each other in terms of the generic object of encroachment), each of which is a separate criminal law norm containing an independent corpus delicti. The provisions of Part 4 determine which socially dangerous acts are crimes, and what penalties are provided for their commission. In our opinion, Part 4 should contain the following mandatory sections, the details of which are still subject to legal design, namely: crimes involving the use of AR\VR technologies (all types of jurisdictions); crimes against man, humanity, peace (all types of jurisdictions); war crimes using AR/VR technologies (all types of jurisdictions); crimes of the scope of application of electronic subjects, electronic objects of avatars or electronic humanoids; crimes in the field of blockchain, AI, cryptocurrencies, and other virtual reality technologies; Metaverse cybercrimes; Metaverse identity crimes; crimes in the field of virtual property, virtual and intellectual property, trademarks, copyrights; crimes against the Metaverse; crimes in the field of ethics; crimes related to the distribution of drugs, weapons, child pornography, emotional violence; crimes based on racial, national, religious, linguistic and other types of enmity, etc.

The last, fifth part is intended for the formation of instructions, interpretations, algorithms, procedures and other issues of law-making activities, which is aimed at standardising law-making processes in the field of electronic jurisdiction Metaverse,

formalising the processes of introducing new regulations, additions, amendments, application of archaic, national, cross-border norms of law, etc.

It is quite obvious that social relations in the Metaverse are different from the traditional ones inherent in the analog world. Electronic social relations are at the stage of creation and initial formation. At present, it is difficult to foresee the whole range of legal problems that need to be settled by various branches of law, including criminal law. However, with some experience formed in the era of Web 1.0-Web 2.0, legal scholars and lawmakers can form a basic vision of the model of the digital Criminal Code Metaverse for further development and adaptation in accordance with the formation of virtual spaces.

New torts and their consequences for the subjects and objects of the virtual world appear. The emergence of new entities such as avatars, electronic humanoids, electronic objects such as cryptocurrency, virtual land, virtual real estate, virtual intellectual property rights, etc., requires new legal approaches and a comprehensive analysis of legal problems in the Metaverse and effective proposals for solving them. The development of digital jurisdiction and the Metaverse Model Digital Criminal Code is one such solution that can help create a legal framework for regulating public relations in virtual environments and create a new legal landscape.

This requires legal researchers and scientists from various fields to combine approaches to the legal regulation of various spheres of human life, especially those social relations that are created today using Metaverse technologies.

The Metaverse Digital Criminal Code is a complex and expanded legal framework that aims to prevent, investigate, and prosecute criminal activity that takes place in virtual worlds. As the use of information and communication technologies continues to grow, the need for a comprehensive legal framework to regulate crimes in the virtual world is becoming an increasingly important part of our understanding of crimes in the virtual world and their impact on society. Legal regulation of the Metaverse still needs a lot of work and research.

So, in view of the above, we state that digital jurisdiction as a new legal paradigm is already an approximate reality. The study confirms that Digital Jurisdiction is not just a derivative of information law, but an independent systemic category that combines legal, technical, ethical and managerial components. It forms its own contour of normative autonomy — a special area of law within which new social relations arise, digital actors, algorithmic institutions and smart contracts operate that perform a regulatory function, replacing or supplementing classical legal procedures.

The digital jurisdiction model is a structural legal model consisting of four interrelated levels. This model provides an opportunity to implement the concept of digital law-making through the use of smart contracts, modular updating of norms and ensuring cross-border interoperability of legal systems. Its implementation will contribute to the formation of a universal legal space Metaverse, within which dispute resolution, protection of rights and legitimation of actions will be carried out electronically.

Digital jurisdiction appears not only as an object of scientific research, but as a tool for civilisational renewal of law, capable of integrating humanistic values into the logic of artificial intelligence and transforming the legal order into a flexible, transparent and self-regulating system.

5.7. Strategic Directions of Ukraine's Integration into the Digital and Legal Space of the European Union Web 4.0: Regulatory Foresight

5.7.1. The strategy of Ukraine's digital integration into the legal space of the European Union

The strategy of Ukraine's digital integration into the legal space of the European Union cannot be built on the principle of reactive adaptation, i.e. the mechanical transfer of already adopted EU acts into national legislation. Instead, it requires proactive legal thinking — regulatory foresight that allows you to outline regulatory horizons, define institutional architecture and formulate a roadmap for legal reforms, taking into account both Ukraine's own legal potential and the dynamics of the formation of EU digital law.

Regulatory foresight in the field of Web 4.0 is a methodological tool that combines legal analysis of technological trends, comparative research of regulatory models and regulatory design of future legal regimes. Its application in the context of this study allows us to formulate specific strategic recommendations for Ukraine aimed at achieving compatibility of its legal system with the EU acquis in the field of digital law, preserving digital sovereignty and ensuring legal protection of citizens in immersive and AI-native environments.

This section is synthetic: it summarises the conclusions of the previous parts of the dissertation research on the legal ontology of the Metaverse, digital identity and subjectivity, regimes for regulating virtual assets and intellectual property, as well as models of digital jurisdiction, the Digital Code and the Digital Criminal Code, and projects them into the plane of specific legal mechanisms of the European integration vector.

Conceptual Foundations of Web 4.0 Regulatory Foresight in Ukraine

Regulatory foresight as a methodological framework is based on three interrelated principles: anticipation — the ability of the legal system to respond to technological changes before their large-scale spread; adaptability — the ability of legal norms to flexibly transform in accordance with changes in the technological landscape; and constructiveness — the ability of law not only to limit technological development, but also to actively create conditions for its legitimate, humanistically oriented deployment.

For Ukraine, the regulatory foresight in the field of Web 4.0 should be based on three key conceptual prerequisites.

Firstly, it is necessary to recognise Web 4.0, Metaverse and AI-native systems not just as technological phenomena, but as a new type of socio-legal reality, where autonomous legal relations arise that require a special legal regime.

Secondly, it should be assumed that Ukraine's European integration vector in the field of digital law is not an alternative to its own rule-making, but a framework condition that determines quality standards and the direction of legal reforms.

Thirdly, the regulatory strategy should be comprehensive: it should cover not only sectoral legislation, but also the constitutional and legal foundations of the digital state, the institutional architecture of digital regulation and the international legal dimension of Ukraine's participation in the formation of global digital standards.

It should be emphasised that Web 4.0 differs significantly from previous waves of digital development, as it involves the deep convergence of the physical and digital worlds through AI-native architectures, semantic Internet, ubiquitous computing, and

immersive presence. This means that traditional legal categories — jurisdiction, legal personality, property, responsibility — are undergoing a qualitative transformation, and not just quantitative complication. Regulatory foresight must take into account this qualitative leapfrogging change and form new legal structures, not just adapt old ones.

In this context, Ukraine has a unique opportunity — and at the same time an obligation — to become not just a recipient of EU regulatory decisions, but an active participant in the formation of international digital law. The wartime experience in the field of digital governance, the large-scale development of the Diia ecosystem, the developed IT industry and the European integration vector, combined with the absence of blocked regulatory traditions in the field of Web 3.0/4.0, create conditions for a legal "leap" — an opportunity to form an advanced regulatory architecture, bypassing intermediate, already outdated solutions.

Regulatory Gap Analysis: Ukraine and EU Digital Law

The analysis of the current legal body of Ukraine and the EU acquis in the field of digital law allows us to identify a systemic regulatory gap that covers several interrelated dimensions.

The first dimension is definitional: Ukrainian legislation does not contain clear, systematic definitions of the basic categories of digital law — "digital", "electronic", "Metaverse", "digital jurisdiction", "AI-native environment", "digital twin", "avatar as a subject of legal relations". This creates legal uncertainty, which complicates enforcement and reduces the level of legal predictability for participants in digital relationships.

The second dimension is institutional. Ukraine has a specialised regulator in the field of digital technologies – the Ministry of Digital Transformation. However, the issues of Metaverse and Web 4.0 are missing. This deficit is especially critical given the fact that the EU is actively shaping this direction.

The third dimension is normative. A comparative analysis shows that Ukraine has not implemented the key EU digital regulations: AI Act (Regulation (EU) 2024/1689), Data Act (Regulation (EU) 2023/2854, applicable from September 2025), Digital Services Act and Digital Markets Act. In addition, the Law of Ukraine "On Personal Data Protection" needs a significant update to achieve real compatibility with the GDPR. There is no specific regulation on digital assets in the broad sense — the Virtual Assets Act does not provide full coverage of relationships in the Metaverse and Web 4.0.

The fourth dimension is procedural. The current procedural legislation of Ukraine is not adapted to the resolution of disputes arising in the Metaverse and Web 4.0. There are no rules on: the admissibility of digital evidence from blockchain environments and AI systems; the procedure for identifying parties acting through avatars or autonomous agents; the competence of courts in relation to cross-border digital disputes; execution of decisions through smart contracts. This gap is strategically dangerous: without procedural mechanisms, the substantive norms of digital law remain declarative.

The fifth dimension is strategic. Ukraine does not have a comprehensive strategy for the legal regulation of Web 4.0, Metaverse and AI adopted at the level of the Verkhovna Rada or the Cabinet of Ministers, which would cover the horizon of 2026-2035. The absence of such a document makes it impossible to consistently implement legislative reforms, coordinate between the branches of government and form the international position of the state in relevant negotiations.

5.7.2. Strategic recommendations in the field of rule-making and codification

Based on the analysis of the regulatory gap and taking into account the conclusions of the previous sections of the dissertation, we formulate a system of strategic recommendations in the field of rule-making, covering three levels: constitutional, codification and sectoral.

A. Constitutional level: principles of the digital state and digital rights

Recommendation 1. Supplement the Constitution of Ukraine with norms that enshrine the digital sovereignty of the state as a component of state sovereignty in Metaverse\Web 4.0; the right to digital identity as an inalienable human right; prohibition of discrimination on the basis of digital status; the right of citizens to access public services in digital form, etc. Appropriate constitutional changes are necessary for digital law to acquire a solid constitutional foundation, and not to remain a set of sectoral norms without a systemic value core. The experience of Estonia, which has enshrined digital rights at the constitutional level, and Finland, which constitutionally guarantees the right to access the Internet, confirms the practicality of this approach.

Recommendation 2. Develop and adopt the Declaration of Digital Rights of Ukrainian Citizens, a document that will not have the force of law, but will consolidate the state position on the balance between innovation and human rights in the digital environment. The declaration should cover: the right to explain automated decisions, the right to digital heritage, the right to be forgotten in AI systems, the right to the protection of the digital twin and avatar, the right to equal access to Metaverse spaces. Such a document will perform a regulatory and signalling function and serve as a guide for the legislator and the courts when interpreting the norms of digital law.

B. Codification level: Digital Code of Ukraine

Recommendation 3. Initiate the development of the Digital Code of Ukraine, a systemic legislative act that codifies the norms of digital law and forms a unified regulatory architecture for Web 4.0, Metaverse, AI systems, and related digital relations. As justified in subsection 5.5 of this dissertation, the structure of the Digital Code should be modular and cover:

General part: basic definitions (Metaverse, digital, electronic, digital identity, avatar, digital twin, AI-native environment, digital jurisdiction, smart contract, autonomous agent); principles of digital law; subjects of digital legal relations and their legal status; objects of digital rights and their classification.

Special part: legal regime of digital assets and virtual property; the mode of circulation and protection of AI-generated content; the mode of personal and biometric data in the Metaverse; the regime of smart contracts and automated transactions; digital responsibility regime.

Procedural part: electronic proceedings; the procedure for submitting and examining digital evidence; peculiarities of dispute resolution with an international digital element; execution of decisions in the digital environment.

International part: mechanisms for recognition and implementation of foreign digital solutions; the basics of digital jurisdiction in the cross-border space; the procedure for interaction with international digital institutions.

Recommendation 4. In parallel with the development of a full-fledged Digital Code, adopt the Law of Ukraine "On the Basics of Legal Regulation of the Digital Environment" as a transitional normative act that will establish the basic principles, definitions and requirements for participants in digital relations until the completion of the codification process. This approach will avoid the regulatory vacuum that may arise if the work on the Digital Code is delayed, and will provide legal certainty for entities already operating in Web 4.0 environments.

C. Sectoral level: priority legislation

Recommendation 5. Adopt the Law of Ukraine "On Artificial Intelligence", built on the risk-based architecture of the EU AI Act, taking into account the specifics of Ukraine. The law should cover: classification of AI systems according to the level of risk; requirements for transparency, accountability and explainability; responsibilities of AI developers and providers in the public and private sectors; banning manipulative AI practices in immersive environments; the mechanism of the supervisory authority with the authority to assess compliance.

Recommendation 6. Significantly update the Law of Ukraine "On Personal Data Protection" in the direction of real harmonisation with the GDPR and their expansion in relation to the specifics of the Metaverse: introduce a special mode for processing biometric and neural data collected in XR environments; to establish increased requirements for obtaining informed consent in immersive environments where cognitive biases are technologically reinforced; determine the legal status of behavioural and emotional data generated in the Metaverse; establish requirements for minimising data and limiting its use in AI training without explicit consent.

Recommendation 7. Develop the Law of Ukraine "On Digital Markets and Digital Services", integrating the EU DSA and DMA approaches, taking into account the peculiarities of the domestic market. Particular attention should be paid to: obligations for operators of Metaverse platforms regarding the transparency of algorithms, content moderation and protection of user rights; measures against the monopolisation of the digital gateway market; mechanisms to ensure the interoperability of platforms and the portability of data and digital assets; prohibiting discriminatory practices against third-party content and service providers.

Recommendation 8. To make systemic changes to the Civil Code of Ukraine in terms of regulation of digital objects of civil rights: to consolidate the legal regime of tokenised assets and NFTs as objects of civil circulation; to determine the legal status of smart contracts as a type of civil law agreements with peculiarities of execution; regulate ownership of digital twins and avatars; establish a digital heritage regime — the rights and procedure for inheriting digital accounts, assets, and identities in the Metaverse.

5.7.3. Strategic Recommendations in the Field of Institutional Architecture

Regulatory reforms will remain ineffective without appropriate institutional infrastructure. Preliminary analysis showed that one of the key structural deficits of Ukraine is the lack of specialised bodies capable of carrying out systematic oversight, developing standards and coordinating enforcement in the field of Web 4.0 and Metaverse. The institutional architecture proposed below is phased and takes into account real budget and personnel constraints.

A. National Digital Law and AI Regulator

Recommendation 9. To establish the Agency for Digital Law and Artificial Intelligence of Ukraine (ADCI) — a specialised independent regulator that supervises digital law, Metaverse and AI. The key functions of the ADCI should include: rule-making — development of bylaws, standards and methodological recommendations in the field of digital law; supervisory — monitoring the compliance of digital platforms, AI systems, and Metaverse operators with legal requirements; accreditation — conformity assessment and certification of AI systems by risk categories; coordination — interaction with the relevant EU authorities (European AI Office, EDPB, BEREC) and other regulators.

The structure of the ADCI should be multidisciplinary: lawyers in the field of digital and information law, AI and cybersecurity specialists, digital market economists, and human rights specialists. Ensuring the independence of the regulator from the executive branch is a critical condition for its effective functioning and the credibility of business and civil society in its decisions.

B. Specialised digital justice

Recommendation 10. Introduce specialised digital chambers as part of commercial courts to consider disputes related to the Metaverse, AI systems, smart contracts, and digital assets. As justified in subsection 5.4 of this study, the judicial system of digital jurisdiction should cover: mechanisms for authenticating digital evidence from blockchain environments; the procedure for identifying parties through decentralised identifiers (DIDs); procedures for studying algorithmic decisions as evidence; XR case resolution technology for cross-border disputes.

Recommendation 11. Develop and implement the Digital Justice Rules — a procedural document that establishes the specifics of proceedings in cases with a digital element: standards for the admissibility and evaluation of digital evidence; requirements for forensic IT experts; the procedure for interaction with foreign digital courts and arbitrations; rules for executing decisions through smart contracts and in the digital registry.

C. Regulatory Sandbox for Web 4.0

Recommendation 12. Introduce a regulatory sandbox mechanism for Web 4.0 and Metaverse — a controlled environment for testing new digital technologies and business models in the context of a temporary relaxation of certain regulatory requirements under the supervision of the ADCI. This approach, provided for by the EU Web 4.0 Strategy and the AI Act, allows: to identify regulatory gaps before the large-scale deployment of technologies; to accumulate empirical data for the formation of balanced regulation; to involve innovative startups in the process of forming norms; reduce regulatory barriers to entry without weakening the protection of rights.

Recommendation 13. To establish the National Digital Law Laboratory (NLRC) as a scientific and applied institution at the ADCI, which will carry out: legal foresight in the field of Web 4.0 and AI; development of model bills; comparative legal research; training of specialists of a new generation — lawyers, architects of law of the digital age. The laboratory should be open for cooperation with universities, IT companies and international partners, in particular with the JRC (Joint Research Centre) of the European Commission and ENISA.

5.7.4. Legal mechanisms of Ukraine's integration into the EU digital space

Ukraine's digital integration into the EU legal space is a multidimensional process that includes not only approximation of legislation, but also participation in the formation of EU digital law, mutual recognition of digital solutions and interoperability of digital infrastructures. The legal mechanisms of this process are systematised below according to four vectors.

A. Approximation of legislation and implementation of the acquis

Recommendation 14. To develop and approve a detailed "Digital Plan" for approximation of Ukrainian legislation to the EU acquis in the field of digital law for 2026-2036, with clear deadlines, responsible authorities and implementation criteria. The priorities for implementation are: AI Act (EU Regulation 2024/1689); Data Act (EU Regulation 2023/2854); DSA and DMA; eIDAS 2.0 Regulation (2024/1183) on the European Digital Identity System; MiCA in the part related to the Metaverse economy; NIS2 Directive on Cybersecurity.

Recommendation 15. To approximate legislation not by the method of direct translation and reproduction of EU acts, but by the method of interoperability — to determine the functional requirements and results of regulation and to ensure their achievement by legal means that correspond to the legal tradition of Ukraine. This approach, recommended by the Venice Commission for EU aspirant countries, avoids the mechanical transfer of norms that are not adapted to the recipient's legal system and preserves one's own legal identity.

B. Digital Identity and Mutual Recognition: Integration to eIDAS 2.0

Recommendation 16. To ensure the technical and legal compatibility of the Electronic Identification and Authentication System (BankID, Mobile ID, Diia.Signature) with the Architecture and Reference Framework of the EU Electronic Wallet (EUDIW) provided for by the eIDAS 2.0 Regulation. This is a condition for the recognition of the digital identities of Ukrainian citizens in the EU member states and the mutual recognition of digital signatures. In the context of Metaverse and Web 4.0, such interoperability is especially critical: it ensures the legal significance of the actions of Ukrainian users in cross-border Metaverse environments.

Recommendation 17. Legislate the legal status of decentralised identifiers (DIDs) and verifiable credentials as alternative forms of digital identity compliant with the W3C DID Core Specification and eIDAS 2.0 standards. This will allow Ukrainian entities to use Web 3.0/4.0-compatible forms of identification in legal relations arising in decentralised Metaverse environments, while maintaining the legal significance of their actions.

C. Ukraine's participation in the formation of EU digital standards

Recommendation 18. Ensure Ukraine's active participation in the work of the technical committees ETSI, CEN/CENELEC and ISO, which develop standards in the field of Web 4.0, Metaverse, AI and digital identity. The status of an associate member of the EU opens up appropriate opportunities for participation in the formation of standards at the project level, and not only their adoption as fait accompli. The development of common standards is strategically important: in Web 4.0, "who writes the standard determines the law."

Recommendation 19. Join the initiative of the European Commission to form the "EU Standardization Agenda for Web 4.0 and Metaverse" and propose draft standards in areas where Ukraine has competitive advantages: cybersecurity in conditions of active conflict (combat cyberspace as a testing ground for the development of protection technologies), digital evidence in emergency situations, remote justice and e-governance in extreme conditions.

D. International Digital Jurisdiction: Contractual Mechanisms

Recommendation 20. Develop and ratify bilateral agreements on the mutual recognition of digital solutions and documents with EU Member States, based on the model of cross-border digital jurisdiction based on subsection 5.4 of the dissertation. Such agreements should cover: mutual recognition of electronic signatures and digital documents; enforcement of decisions of digital courts and arbitrations; exchange of digital evidence in criminal and civil cases; collaborative investigation of cyber incidents and digital crimes in the Metaverse.

Recommendation 21. Ratify and implement the Second Additional Protocol to the Budapest Convention on Cybercrime (2022), which regulates cross-border access to computer data for criminal justice purposes and contains provisions on stored electronic evidence. Ratification of this document is critical to the investigation of cybercrime in the Metaverse and Web 4.0, where evidence by definition crosses jurisdictional boundaries.

Regulatory Foresight of Web 4.0: Horizons 2026–2035

Regulatory foresight in the field of Web 4.0 involves not only responding to the current state of technology, but also anticipatory regulatory design based on the analysis of technological trends and their legal consequences. Based on the study, we determine three time horizons of regulatory foresight for Ukraine.

Horizon 1 (2025–2027): Laying the foundation

On the first horizon, the priority is to address the most critical regulatory gaps and lay the institutional and regulatory foundation for further development. Key activities: adoption of the Law "On Artificial Intelligence" and the updated Law "On Personal Data Protection"; the formation of ADCI and the introduction of a sandbox for Web 4.0; ratification of the Second Additional Protocol to the Budapest Convention; harmonisation of the digital identification mode with eIDAS 2.0; the beginning of the development of the Digital Code of Ukraine.

Horizon 2 (2027–2030): Building Digital Jurisdiction

On the second horizon, Ukraine should move from reactive adaptation to the active development of digital jurisdiction. According to the model substantiated in subsections 5.3–5.4 of this dissertation, we are talking about: adoption of the Digital Code of Ukraine; the introduction of digital chambers in commercial courts and the Digital Justice Regulations; concluding bilateral agreements with EU member states on the mutual recognition of digital solutions; participation in shaping the EU agenda for Web 4.0; phased integration into the EU Digital Single Market within the framework of the association process.

Horizon 3 (2030–2035): Digital sovereignty and global role

On the third horizon, Ukraine should strive for the status of a full-fledged participant in the global digital legal order with its own normative voice. Key objectives: full integration into the EU Digital Single Market (in case of completion of the EU accession

process or within the framework of associate status); participation in initiatives to develop the UN Convention on Digital Law and Legal Regulation of AI; promotion at the international level of models of digital jurisdiction and the Digital Code of Ukraine as role models; formation of regional digital legal leadership in Central and Eastern Europe.

In the context of the third horizon, issues that are still on the sidelines of the regulatory discussion, but already require foresight reflection, are of particular relevance. Among them are the legal status of autonomous AI agents and their civil and criminal liability; regulation of neural interfaces and neural data in Web 4.0 systems; the legal regime of "digital immortality" — the preservation and use of digital copies of a person after his death; DAO governance of public goods and decentralised governance in the Metaverse; quantum-protected evidentiary protocols and their place in procedural law.

5.7.5. Implementation Mechanism: Roadmap for Legal Reforms

The strategic recommendations set out in this section require a specific implementation mechanism, which includes not only a list of legislative initiatives, but also the organisational conditions for their implementation, monitoring and correction mechanisms.

The first step is the adoption of the Concept of State Policy in the Field of Web 4.0, Metaverse, a document of the Cabinet of Ministers of Ukraine that defines the strategic goals, principles and priorities of regulation in this area for the horizon of 2026-2036. The concept should become a starting point for all subsequent legislative initiatives and ensure their systemic coherence.

The second step is the establishment of an Interagency Working Group on Digital Law and Web 4.0 with the participation of the Ministry of Digital Transformation, the Ministry of Justice, the NBU, the Security Service of Ukraine, the Prosecutor General's Office, the High Council of Justice and leading academic institutions. The task of the working group is to coordinate the development of draft laws, ensure their coherence and synchronisation with relevant EU initiatives.

The third step is the introduction of mandatory digital legal expertise of draft laws, similar to anti-corruption and gender-legal examinations. Any draft law relating to digital relations, AI systems, data, or the Metaverse must be assessed for compliance with the principles of digital law, compatibility with the EU acquis, and implications for human rights in the digital environment.

The fourth step is the development of digital legal education as a systemic component of legal education in Ukraine. It is necessary to introduce mandatory disciplines "Digital Law", "Metaverse and Web 4.0 Law", "AI Legal Regime" in the programs of law faculties; to introduce the specialisation "Digital Law Lawyer" at the master's and postgraduate levels; develop advanced training programs for judges, prosecutors and investigators in the field of digital evidence and AI systems.

Special context: digital law of Ukraine under martial law and post-war reconstruction

No digital law strategy for Ukraine can ignore the unique context in which it is being formed: the ongoing armed conflict, the large-scale destruction of physical and digital infrastructure, the forced displacement of millions of citizens, and the needs of post-war reconstruction. This context, on the one hand, complicates the implementation of strategic reforms, and on the other hand, it forms unique conditions and needs that can become the engine of legal innovations.

First, Ukraine has gained unprecedented experience in the field of digital governance in times of crisis: the functioning of state registers in the face of cyberattacks, the evacuation of digital assets, management through the Diia ecosystem under martial law, and the digital identification of internally displaced persons. This experience is invaluable for the development of digital resilience standards, which should become part of the regulatory development for the EU and the international community.

Secondly, post-war reconstruction is a chance for a "legal leap": the restoration of destroyed infrastructure and institutions can be carried out immediately according to Web 4.0 standards and EU digital law, without the need to modernise outdated systems. Digital property registers, digital courts, AI-assisted reconstruction management — all these solutions can be implemented as "greenfield" projects embedded in the latest legal framework.

Thirdly, the collection of evidence of war crimes in the context of Web 3.0/4.0 has formed a unique practice of using blockchain fixation, open intelligence (OSINT), and AI analysis in criminal justice. The legal legitimisation of this evidence in international courts is an urgent task, which is both a need of today and a laboratory for shaping future standards of digital evidence in Web 4.0.

Recommendation 22. Adopt the Law of Ukraine "On Digital Evidence and Digital Forensics", which will systematically regulate the procedure for collecting, fixing, storing and using digital evidence from blockchain systems, AI environments and Metaverse in judicial proceedings. This law should take into account the experience gained in documenting war crimes and ensure compatibility with the international standards of evidence of the ICC and other international judicial institutions.

Summing up, it is established that there is a systemic regulatory gap between the existing legal regulation of Ukraine and the EU acquis in the field of digital law, covering definitional, institutional, regulatory, procedural and strategic dimensions. Closing this gap requires a comprehensive approach that goes beyond the mechanical approximation of legislation.

The regulatory foresight of Web 4.0, developed within three time horizons (2025–2027, 2027–2030, 2030–2035), defines the sequence of priorities and allows for the implementation of legal reforms systematically rather than reactively. The key methodological basis is the combination of anticipation, adaptability and constructiveness of legal regulation.

It is proved that Ukraine, despite the complexity of the current context, has a unique opportunity to make a legal "leap" in the field of digital law: bypassing outdated regulatory decisions, to form an advanced Web 4.0 regulatory architecture that is compatible with the EU legal space and open to participation in the formation of global digital standards. The realisation of this potential requires not only legislative will, but also the formation of a new generation of lawyers-designers of the digital age — specialists who are able to think in terms of norms, code, and technological architectures at the same time.

The strategic recommendations and regulatory foresight proposed in this subsection are a specific scientific and practical contribution of the dissertation research to the formation of the doctrine of digital law of Ukraine and can serve as a direct basis for legislative initiatives, strategic documents of the Cabinet of Ministers and scientific research in related fields.

AFTERWORD

The genesis of the legal regulation of the Metaverse and Web 4.0 technologies as a juridical concept reveals a distinct developmental sequence, shaped by a set of determinative factors that have driven, and continue to drive, the transformation of legal reality throughout the process of digital evolution. The identification of the principal stages of this genesis is inseparable from the recognition, within international and regional law, of digital environments as an autonomous subject of legal regulation in their own right. This makes it possible to trace a trajectory that runs from the earliest conceptions of digital relations articulated within the confines of classical branches of law, through their acquisition of independent normative significance, to the present stage, at which digital law attains doctrinal autonomy vis-à-vis classical sectoral formations — a development that follows logically from the post-anthropocentric transformation of social relations.

The delineation and critical examination of the theoretical, legal, and methodological foundations, together with the bibliographic and normative basis of this study, have revealed the multiplicity and pluralism of existing and possible interpretations of Metaverse regulation. This plurality necessitated the elaboration and application of an interdisciplinary conceptual approach capable of reconciling technological and anthropological perspectives, evolutionary and, potentially, revolutionary orientations, practical-legal and theoretical-legal viewpoints, and both established and emergent contributions of contemporary scholarship and practice. The approach advanced here rests on legal constructivism, a post-anthropocentric ontology, and a synergetic model of regulation, within which legal norms, software code, platform architecture, and algorithmic governance operate in conjunction as a single system of normative influence.

The disclosed multi-aspect nature of digital social relations within the Metaverse has made it possible not merely to examine their functional significance from various perspectives within the legal system, but also to investigate the points of convergence and divergence between digital and classical legal relations — their technological form as distinct from their social substance — and to differentiate between relations that are digital in form and relations that are digital in substance. This distinction advances the inquiry beyond the confines of classical legal personhood toward the legal status of algorithmic agents and autonomous artificial intelligence systems.

The distinctiveness of this monograph's treatment of the legal regulation of immersive technologies lies, above all, in the construction of a coherent and self-sufficient conceptual-categorical apparatus that resolves the terminological indeterminacy characteristic of existing scholarly and normative approaches. A synthesis of the prevailing pluralism of approaches has permitted the formulation of original definitions of the foundational categories without which further analysis would be untenable: the Metaverse is defined as an autonomous socio-technological environment of a new type, within which specific digital social relations are constituted through the convergence of immersive interfaces, decentralised network architectures, algorithmic artificial intelligence systems, and autonomous forms of digital organisation; digital social relations are defined as a qualitatively new type of legal relationship in which legally significant acts are performed not through the direct expression of a subject's will, but through algorithmically mediated environments, scenarios, and interaction protocols;

algorithmic action is defined as a legally relevant event arising from the automated execution of programmed scenarios without direct human intervention; and digital normativity is defined as the capacity of software code, algorithms, and protocols to perform regulatory functions equivalent to normative prescriptions.

To this same end, the monograph articulates and substantiates a series of original models that constitute the conceptual core of the study. First and foremost, the concept of digital jurisdiction is proposed and scientifically substantiated as an independent legal institution of digital law — a construct premised on the rejection of an exclusively territorial principle, and one that provides for the technological localisation of legally significant acts through the digital identification of subjects, platform architecture, access protocols, algorithmic scenarios, and data-validation mechanisms. This concept is, arguably, the monograph's boldest and, at the same time, most indispensable intellectual contribution: it endows with genuine regulatory substance a space in which the classical mechanisms of state sovereignty are objectively constrained.

The concept of code-based regulation has likewise received further development and attained doctrinal articulation: the legitimisation of software code, algorithms, smart contracts, and access protocols as an autonomous form of normative regulation operating alongside classical sources of law. It is demonstrated that such a regime possesses a coercive character, exerts a genuine effect on the scope of subjects' rights and obligations, and is capable of generating autonomous normative regimes — circumstances that necessitate its doctrinal recognition, legal legitimation, and incorporation into the system of sources of digital law, accompanied by the simultaneous assurance of public oversight, transparency, and the protection of human rights.

A risk-based model of the legal regulation of the Metaverse is proposed and doctrinally substantiated as the foundational principle for the construction of a digital legal order. It is demonstrated that the legal regulation of the Metaverse cannot be premised upon uniform rules applied indiscriminately across all technologies, but must instead differentiate regulatory requirements according to the risk profile of the platforms, algorithms, digital agents, and Metaverse segments in question. This approach reconciles innovative development with the principles of proportionality, preventive protection, legal certainty, and accountability, thereby constituting a flexible and adaptive mechanism of legal influence capable of evolving in step with technological change.

The refinement of the classificatory approach to the subject composition of the Metaverse has yielded a comprehensive doctrinal classification grounded in the combination of formal-legal and functional-algorithmic criteria, encompassing natural persons, legal entities, platform operators, decentralised autonomous organisations (DAOs), infrastructure providers, digital personas, avatars, algorithmic agents, and autonomous artificial intelligence systems. It is argued that legal personhood within the Metaverse is not exclusively anthropocentric but functional and delegated in character, contingent upon a given participant's capacity to perform legally significant acts and to exert influence upon digital processes — thereby transcending the limitations of the classical theory of the legal subject.

The conception of the objects of digital legal relations within the Metaverse has been expanded and doctrinally reconsidered through their differentiation from classical objects of property, non-proprietary, and informational character. It is demonstrated that digital

identities, avatars, digital twins, virtual spaces, tokenised assets, algorithmic models, and the outputs of artificial intelligence systems possess a hybrid, dynamic, and processual nature: they combine elements of information, functionality, behavioural scenarios, and legal status, all of which change in real time. This circumstance necessitates the formulation of special legal regimes that transcend the classical dichotomy of "thing" versus "information."

The concept of distributed (multi-tiered) legal liability within the Metaverse is substantiated as a doctrinally novel model of response to unlawful conduct within immersive and algorithmically governed environments. The analysis undertaken demonstrates that the classical model of personalised liability is functionally inadequate wherever harm results from the joint and interrelated conduct of a human actor, platform operators, algorithm developers, infrastructure providers, DAOs, and autonomous artificial intelligence systems. The proposed approach, whereby liability is apportioned according to the degree of algorithmic autonomy, the character of the delegation of authority, and the risk profile of the participant concerned, secures a balance between the innovative development of the Metaverse and the principles of justice and the effective protection of human rights.

A separate, strategically significant component of the monograph lays the conceptual, methodological, and structural foundations of a Digital Code of Ukraine as a systemic codificational instrument of a new generation. It is argued that a digital code cannot be reduced to a compilation of discrete norms of information or IT law, but must instead be constructed as a modular, dynamic, and technologically neutral codificational system integrating provisions on digital jurisdiction, digital identity, algorithmic systems, artificial intelligence, immersive technologies, digital subjects and objects, distributed liability, and risk-based regulation. An original model of the phased codification of digital law is proposed — proceeding from the formulation of foundational principles, terminology, and general provisions to the institutionalisation of discrete sectoral modules — thereby ensuring adaptability, coherence with European and international standards, and the minimisation of normative instability.

Against the background of an examination of social and technological transformations, the monograph identifies and analyses the determinants underlying the emergence of a new digital legal order. It concludes that a doctrinal reconsideration of the role of the state is an indispensable condition for the effective legal regulation of the Metaverse. Under conditions of decentralised platforms, autonomous algorithmic systems, and transnational immersive environments, the state cannot effectively discharge its functions through prohibitive-permissive mechanisms alone. Its principal role, rather, consists in the establishment of legal and technological frameworks (rules by design), the imposition of mandatory standards, the assurance of interoperability, and the supervision of algorithmic governance, without direct intervention in every technological process. A direct connection is likewise demonstrated between the legal regulation of the Metaverse and questions of Ukraine's digital sovereignty and national security — a connection that, in present circumstances, constitutes not an academic abstraction but a practical necessity.

Within this context, the challenge of preparing a new generation of legal practitioners assumes fresh significance. The analysis conducted demonstrates that, absent a profound transformation of legal education — one incorporating interdisciplinary knowledge of

artificial intelligence, blockchain architectures, data governance, cybersecurity, and digital ethics — none of the concepts proposed herein will be realised in practice. A concept of preventive digital rulemaking is proposed, combining doctrinal forecasting, experimental legal regimes (regulatory sandboxes), and adaptive normative constructs, as a strategic response to the law's objective incapacity to function in a purely reactive mode under conditions in which the pace of technological change outstrips that of classical lawmaking.

The multiplicity and variability of scholarly interpretations of legal personhood, together with their formalisation in legal instruments, have permitted the proposal and substantiation of the concept of a post-anthropocentric model of law as a new stage in the evolution of legal ontology. This model rests on the recognition of a hybrid regulatory reality, within which legal significance attaches not solely to human conduct but also to algorithmic processes, the architecture of digital systems, and the behavioural scenarios embedded in code. Its application enables a reconceptualisation of the categories of legal personhood, liability, fault, and control, the formulation of adequate legal mechanisms for regulating the interaction of human beings, artificial intelligence, and digital infrastructure, and the establishment of a theoretical foundation for the development of digital law as the law of a post-anthropocentric civilisation.

The conceptualisation of the legal regulation of the Metaverse and digital environments advanced in this monograph represents a particular — albeit fundamentally significant — stage in their theoretical-legal comprehension. The author is convinced that it must be refined in the course of further scientific and technological development, while nonetheless serving already today as a practical point of reference for the legislator. The scholarly paradigm thus articulated reflects a transition from reactive, sectorally fragmented law toward projective, systemic, and preventive legal thinking capable of accompanying the development of the Metaverse, artificial intelligence, and decentralised digital infrastructures. It lays the theoretical and methodological groundwork for further scholarly inquiry, lawmaking, and the formation of digital legal statehood amid global digital transformation. The construction of a digital legal order is a shared intellectual and civilisational undertaking, within which law, technology, and human dignity must find a new equilibrium — one capable of withstanding the trial of time.

APPENDICES

Legal Typologies of Metaverse, DLT and AI Governance

English translation — author's typology tables

Table 1. China: Regulatory Approach

(author's typology)

Regulatory Contour	Key Goal	Typical Instruments	Regulated Objects
Cybersecurity & National Security	Risk control, evidentiary capacity, accountability	Obligations for network operators; cooperation with security authorities	XR platforms, servers, event logs, identification
Data & Privacy	Minimization of misuse, control over sensitive data	"Sensitive data" regime; legitimate-purpose requirements	Biometrics, body/face/voice tracking, spatial maps
Content & Algorithms	Manageability of the information environment	Rules for recommendation algorithms and synthetic content	Avatars, deepfakes, moderation, "digital plausibility"
Digital Assets & Economy	Financial stability, control of speculation	Restrictions/bans on crypto circulation	Token/NFT economies, "play-to-earn", virtual markets

Table 2. Legal Stratification of Metaverse Infrastructure

(author's typology)

Layer Name	Key Actors (Operators)	Legal Facts and Objects	Specific Risks	Legal Regulation Regimes	Evidentiary & Procedural Requirements
Identity Layer	Identification providers, trust service providers	Attribution of actions, authentication, subjectivity (avatars, agents), identification data	Anonymity, pseudonymity, tortious capacity, attribution problems	Digital jurisdiction; rules for collecting and auditing identification data	Reliable attribution for evidence and dispute resolution
Data Layer	Hosting providers, data controllers	Personal data, sensor and behavioural data (biometrics), trade secrets	De-anonymisation, privacy breaches, secondary use of data	Personal data protection, cybersecurity, data minimisation, access control	Operation logging, procedures for exercising data-subject rights, machine interoperability
Content Layer	Platforms, moderators, creators (human and AI)	Intellectual property objects, user/platform content, deepfakes	Defamation, hate speech, copyright infringement, manipulation	Notice-and-action, IP regimes, moderation rules	Transparency of moderation, establishing authorship and fact of distribution

Layer Name	Key Actors (Operators)	Legal Facts and Objects	Specific Risks	Legal Regulation Regimes	Evidentiary & Procedural Requirements
Transaction Layer	Marketplaces, payment providers	Virtual assets, tokens, smart contracts, digital access rights, licences	Fraud, code errors, money laundering (AML)	AML/CFT procedures, KYC, consumer protection, civil-law regimes	Threshold criteria, transaction-dispute rules, compliance control
Evidentiary Layer	Technical auditors, platforms (logging functions)	Digital traces, logs, metadata, cryptographic hashes	Evidence manipulation, procedural uncertainty, loss of integrity	Integrity and immutability standards, chain of custody	Timestamping, attestation, evidence export/import procedures
Sanctions Layer	Private platform operators	Blocking, access restrictions, deplatforming	Unlawful sanctions, privatised justice, discrimination	Procedural legitimacy, appeal, algorithmic transparency, proportionality	Notification of grounds, right to explanation, complaint-review timelines

Table 3. Compliance Map

(author's typology)

Technical Function	Legal Function	Legal Regime / Institution	Risks	Compliance / Safeguards
Data hashing	Ensuring evidentiary integrity	Electronic evidence; integrity standards	Substitution of "input" data before hashing	Source-fixation procedures; chain of custody
Timestamp / block time	Proving the moment a fact existed	Proof of time; priority of rights	Time manipulation in some protocols	Recognized time sources; cross-verification of events
Consensus (PoW/PoS/etc.)	Legitimizing ledger state	Determining "finality" for evidence	Reorganizations, attacks, MEV	Finality policies; anti-MEV mechanisms; validator audits
Ledger publicity	Transparency of asset circulation	Public control, fraud prevention	De-anonymisation; personal-data leaks	Pseudonymization; data minimisation; permissioned layers
Permissioning (access roles)	Defining responsible persons	Licensing/oversight; governance	Concentration of power; censorship	Access regulations; independent audit; appeal procedures
Tokenization	Objectifying rights in digital form	Virtual assets; claims	Substituting legal title with a "token"	Rules on title/collateral; disclosure requirements
Smart contract	Automated execution of terms	Contract law; digital agreements	Code errors; irreversible losses	Formal verification; emergency pauses; risk insurance
Oracles (external data)	Linking on-chain data to reality	Evidentiary value of off-chain events	Oracle manipulation	Source certification; multi-channel oracles; provider liability
DID/VC integration	Attributing actions to a subject	Digital identity	Key theft; attribute forgery	KMS policies; access recovery; attribute revocation
Reputation protocols	Trust between pseudonyms	"Soft" enforcement	Reputation gaming; collusion	Anti-Sybil measures; proof of participation; reputation-algorithm audits

Technical Function	Legal Function	Legal Regime / Institution	Risks	Compliance / Safeguards
Cross-chain / interoperability	Mutual recognition of states	Legal interoperability	Bridges as attack points; rule collisions	Bridge standards; certification; insurance funds
On-chain escrow	Ensuring performance	Securing obligations	Wrongful asset lock	Dispute procedures; multisig; judicial/arbitration trigger
Smart-contract event logs	Tracing execution	Evidence of performance/non-performance	Lack of context on "what it actually meant"	Normative semantics of events; legal event ontology
Protocol versioning	Legitimacy of rule changes	Decentralized governance	"Silent" changes, forks	Public RFCs; voting; due process for upgrades
Cryptographic signatures	Non-repudiation of intent	E-signature; trust services	Key compromise	Rotation policies; hardware modules; qualified services

Table 4. Comparative Matrix of DLT/Crypto-Asset Regulatory Strategies

(author's typology)

Jurisdiction	Dominant Approach	Primary Regulatory Focus	Institutions / Mechanisms	Key Risks to Rights / Innovation
EU	Techno-neutral	Crypto-asset markets + DLT pilot infrastructure	MiCA Regulation, DLT Pilot Regime	Compliance complexity, "entry barrier"
USA	Financial-risk-based (polycentric)	Oversight, securities/services, AML	SEC / CFTC / FinCEN + state regimes	Fragmentation, legal uncertainty
United Kingdom	Hybrid (financial + new regulated activities)	Regulated crypto-asset activities	HMT legislation, FCA/BoE	Delayed implementation, compliance costs
Singapore	Financial-risk-based (strict licensing)	DTSP licensing, stablecoin stability	FSMA regime, MAS	Restricted access for small innovators
Switzerland	Techno-neutral (private-law adaptation)	"Ledger-based securities"	DLT Act, private-law instruments	Regulatory arbitrage, complexity of title
Canada	Financial-risk-based	Registration/oversight (MSB)	FINTRAC registration	Compliance burden
Australia	Hybrid (platform oversight)	Regulation of digital-asset platforms	Treasury consultations/models	Transitional regulatory uncertainty
China	State-controlled	Ban/restriction of virtual currencies	Banking-financial and law-enforcement mechanisms	Narrowing of rights, shadow-economy growth
Japan	Financial-risk-based	Exchange registration / stablecoins	FSA oversight	High entry barriers
Ukraine	Transitional (emerging)	Virtual-asset market model + taxation	Draft laws + regulator concepts	Risk of fragmentation and delay

Table 5. DAO Architecture

(author's typology)

Level	Layer Name	Content in the Metaverse
1	Infrastructure	Blockchain, network protocols, storage
2	Smart contracts / logic	Voting rules, treasury, asset markets
3	Tokens & economy	Governance tokens, utility tokens, NFT assets
4	Governance	Voting (often token-weighted), delegation, multi-level procedures
5	Socio-legal level	Participants, reputation, legal status, integration with offline law

Table 6. Definitions of the Concept of "Identification"

(author's typology)

No.	Concept, Characteristics, Content
1	The process of collecting, verifying, and establishing the validity of attributes of identification data regarding a specific subject, sufficient to determine and confirm their identification data in a specific context. Synonyms: identity proofing, registration (United Nations, n.d.).
2	A means of establishing: a) a person's identity based on the totality of their general and specific data; b) a system user's authority by means of a password (Verkhovna Rada of Ukraine, 1997).
3	Establishing the fact of use of goods placed under the customs regime of processing within or outside the customs territory of Ukraine, in processed products (State Customs Service of Ukraine, 2003).
4	Identification of an object by its reflections (traces) (Ministry of Internal Affairs of Ukraine, 2005).
5	A procedure for recognising a user in a system, usually by means of a predetermined name (identifier) or other a priori information about them that is perceived by the system (Cabinet of Ministers of Ukraine, 2006).
6	A procedure for recognising a user in a system, usually by means of a predetermined name (identifier) or other information about them perceived by the information (automated) system (Ministry of Justice of Ukraine, 2011).
7	Measures taken by a primary financial-monitoring entity to establish a person's identity by obtaining their identification data, together with the entity's receipt of identification data from the client (or the client's representative) (Verkhovna Rada of Ukraine, 2021).
8	A procedure for using a person's identification data from documents created on tangible media and/or from electronic data, the result of which ensures the unambiguous establishment of a natural person, legal entity, or representative of a legal entity (State Property Fund of Ukraine, 2018).
9	A procedure for recognising a user in the Register by means of a predetermined name (identifier) or other information about the user perceived by the automated information system (Prosecutor General's Office of Ukraine, 2018).

Table 7. Definitions of the Concept of “Identification Data”

(author's typology)

No.	Concept, Characteristics, Content
1	Information about a specific subject in the form of one or more attributes that allow the subject to be sufficiently distinguishable in a given context — a set of a person's attributes that allow that person to be distinguished from other persons in a specific context (United Nations, n.d.).
2	A set of data that makes it possible to unambiguously establish a person, namely: for a natural person — the information specified in the relevant provisions of Article 11 of the Law of Ukraine “On Prevention of and Counteraction to the Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism, and Financing of the Proliferation of Weapons of Mass Destruction”; equivalent provisions apply to a natural person-entrepreneur, a legal entity, and a trust or similar legal arrangement; the list of required data may also be determined by state financial-monitoring entities in cases set out in that Law (Verkhovna Rada of Ukraine, 2020).
3	Data necessary to uniformly characterise a specific item or batch — for example, the material balance area, type of nuclear material, batch identification, material description, and the type and date of change in inventory quantity (State Nuclear Regulatory Inspectorate of Ukraine, 2021).
4	Basic data about an applicant or customer, including full name, place of registration, EDRPOU code / taxpayer registration number or passport series and number (for individuals who, for religious reasons, have refused a taxpayer registration number and have notified the relevant authority accordingly), bank details, contact information, and the legal basis for the authority of the person signing a natural-gas storage (injection/withdrawal) agreement (National Commission for State Regulation of Energy and Public Utilities, 2004).
5	A unique set of data that makes it possible to unambiguously establish a natural person, legal entity, or representative of a legal entity (Verkhovna Rada of Ukraine, 2017).

Table 8. Definitions of the Concept of “Identification Data Management”

(author's typology)

No.	Concept, Characteristics, Content
1	A set of techniques that allow the management of identification, authentication, and authorisation processes for natural and legal persons, devices, and other subjects online (United Nations Commission on International Trade Law, 2015).
2	A set of functions and capabilities (e.g., administration, management and maintenance, discovery, messaging, matching, policy enforcement, authentication, and approval) used to: guarantee information confirming identity (e.g., identifiers, registration data, attributes); guarantee the identity of an entity; and enable commercial and security applications (International Telecommunication Union, 2009).
3	Processes, functions, and capabilities for collecting, verifying, and communicating identification information about a subject to a relying party, so that the relying party can verify the correspondence of that identification information to a specific subject (UNCITRAL Working Group IV, 2014).

Table 9. Definitions of “Identification Data Management / Identity Management”

(chronological overview)

Year	Definition
2001	An identity-management system provides tools for managing all of a person's partial identities in the digital world. A partial identity may or may not uniquely identify a person; for example, a person may use one or more sets of identification data (Clauß & Köhntopp, 2001).
2003	Identity management is a set of business processes and supporting infrastructure for creating, maintaining, and using digital identities (Manders-Huits & Van den Hoven, 2008).
2004	Identity and access management concerns the processes, technologies, and policies for managing digital credentials, as well as individuals' control over access to resources (Chonka et al., 2011).
2007	Identity management provides means for managing and selectively disclosing information about a person relevant to an organisation's users, ensuring privacy needs are met (Del Álamo, 2007).
2008	Identity management is generally understood as the set of processes and tools used to establish the identity of a system user — an employee, customer, contractor, etc. (De Hert, 2008).
2008	Identity management allows the management of a person's identity in two senses: managing the person in physical spaces, and storing complex digital representations of people across multiple databases (Hewitt & Forte, 2008).
2008	Identity-management systems are used to manage users' identification data across multiple systems and to provide users a way to access organisational resources, throughout the user's lifecycle, via single sign-on and credential verification (Tracy, 2008).
2009	Personal-data management is a set of functions and capabilities for administration, management, maintenance, discovery, information exchange, policy enforcement, and authentication, used to secure information about a person and provide tools for managing individual identities in a digital environment (Chadwick, 2009).
2009	Identity management is used to protect user data related to location, interests, and similar attributes, in the digital world in the same way users protect such data in the physical world (Tatli & Lucks, 2009).
2011	Identity management represents a model that provides the right amount of capability at the right time (Olden, 2011).
2017	Identity management is a combination of business processes and technologies used to manage data in IT systems; applications manage data for user objects, attributes, security rights, and authentication factors (IDG Communications, 2017).
2017	Identity management is a broad administrative field concerned with identifying individuals within a system such as a country, network, or organisation, and controlling their access to resources by associating user rights and restrictions with an established identity (TechTarget, 2017).

Table 10. Key US Regulatory Acts in the Blockchain Sector

(federal and state level — author's typology)

Level	Law / Policy	Year	Main Provisions	Regulator / Authority
Federal	Securities Act of 1933; Securities Exchange Act of 1934	1933 / 1934	Regulation of tokens as securities under the Howey test	SEC
Federal	Commodity Exchange Act (CEA)	1936	Recognition of BTC and ETH as commodities; oversight of derivatives	CFTC
Federal	Bank Secrecy Act (BSA)	1970	AML/KYC requirements; registration of exchanges as MSBs	FinCEN
Federal	Digital Commodities Consumer Protection Act (draft)	2022	Separate category of digital commodities; CFTC jurisdiction over digital commodities	US Senate
Federal	Lummis-Gillibrand Responsible Financial Innovation Act (draft)	2022	Comprehensive classification of digital assets as securities or commodities; regulates stablecoins; consumer protection; tax regimes	Senate (Lummis-Gillibrand)
Federal	Executive Order on Digital Assets (repealed January 23, 2025)	2022	Interagency coordination for sustainable development of crypto policy	The White House
Federal	Digital Asset Law	2018–2020	Classification of digital assets; creation of SPDI banks	FinCEN
Colorado	Digital Token Act	2019	Removal of utility tokens from SEC jurisdiction	Colorado General Assembly
Texas	Blockchain Working Group; UCC amendments	2021	Legal recognition of digital assets; legalisation of mining	Texas Blockchain Council
New York	BitLicense	2015	Strict licensing of crypto services; AML policies	New York DFS
California	Executive Blockchain Order (CA EO N-9-22)	2022	Development of rules for NFTs, DAOs, and cryptocurrencies	State of California
Florida	MiamiCoin, Web3 offices	2020–2023	Integration of blockchain into city programs; DAO experiments	City of Miami
Pennsylvania	Toomey Stablecoin Bill	2022	Regulates stablecoins to ensure stability and transparency	Pennsylvania
US House	Digital Trading Clarity Act	2022	Clarifies the definition of digital assets for legal certainty	US House of Representatives
US House	Financial Innovation and Technology for the 21st Century Act	2023	Delineates SEC jurisdiction (restricted assets) and CFTC jurisdiction (additional assets)	US Congress
IRS	IRS Notice 2014-21	2014	Cryptocurrency taxed as property	IRS
Utah	Decentralized Autonomous Organization Act	2022	Regulates DAOs	State of Utah

Table 11. Comparative Table of Regulatory Regimes

(summary of acts, 2010–2025 — author's typology)

Jurisdiction / Law	Regulator & Subject Matter	Licensing / Requirements	Consumer Protection & AML	Innovation & Risks
EU – MiCA (2023)	ESMA/EBA; crypto-assets not previously covered by law	Provider authorisation; token categorisation; transition through 2026	Consumer rights, stablecoin reserves, travel rule	Uniform regulation but high costs; may limit startups
EU – DLT Pilot	ESMA; tokenised financial instruments	Licenses for DLT market infrastructures	Temporary exemptions; limited volumes	Sandbox for innovation, but temporary and capped
USA – CLARITY / FIT21 (drafts)	Division of SEC/CFTC jurisdiction; digital assets	Proposed registration regimes	Investor rights dependent on category	Draft bills; legal uncertainty
China – 2019 Regulations	CAC; blockchain service providers	Registration, real names, security assessment	Ban on illegal content	Tight control; censorship risk
China – 2021 Ban	PBOC; cryptocurrency transactions	Complete ban	Fraud protection	Suppression of innovation
Switzerland – DLT Act 2021	FINMA; tokenised securities	Licenses for DLT trading venues; registered securities	Asset segregation; legal certainty	Increased requirements; new concepts
Singapore – PSA 2019	MAS; digital payment tokens	Licenses for exchanges/wallets; travel rule	KYC/AML; customer protection	Clear rules, but costly
South Korea – AML Act 2020	KoFIU; VASPs	Reporting, real-name bank accounts; licences	Travel rule; suspicious-transaction reporting	Strengthens trust; high costs
Malta – VFA Act 2018	MFSA; VFA offerings/services	Whitepaper; VFA-agent licence	Combats manipulation	High entry barriers
Gibraltar – DLT Regulations 2020	GFSC; DLT providers	Part 7 permission; 10 principles	Asset protection, AML, corporate governance	Flexible approach; requires expertise
Dubai – VA Law 2022 / VARA 2023	VARA; virtual assets	13 rulebooks; VASP licensing	Compliance & risk-management rulebooks	Comprehensive system; difficult for startups
Estonia – AML Act 2022	FIU; VASPs	High licensing fees; statutory capital	Travel rule; detailed reporting	Increases security; burdens small firms
Ukraine – Law "On Virtual Assets" 2022	NSSMC/NBU; virtual assets	Permit for exchange/storage/transfer; 1-year term	Integrity requirements; financial monitoring	Law not yet in force; no tax rules
Japan – PSA/FIEA (2019)	FSA; crypto exchange services	Mandatory registration; capital requirements	Self-regulation, customer protection	High standards; entry barriers
El Salvador – Bitcoin Law 2021	Government; bitcoin	Legal-tender status	Protection undefined	High volatility; law partially repealed

Table 12. Functions

(author's typology)

Technical Function	Legal Function	Legal Regime / Institution	Risks	Compliance / Safeguards
Hashing of a digital object (content)	Object identification, version fixation	Evidence of existence/priority; electronic evidence	Hash collision; file substitution with the same description	Deposit procedures; binding to storage; chain-of-custody audit
Timestamp in DLT	Fixing the time of an event	Evidentiary value of the moment of creation/publication	Client-side time manipulation	Use of trusted timestamps; finality standards
Digital signature / key	Authentication of the subject	Digital identity; electronic trust services	Key compromise; dispute over "who signed"	Qualified/advanced signatures, key policies, rotation, access logs (Ukrainian legislation)
Consensus (PoW/PoS, etc.)	Consistency and immutability of the ledger	Trust in the ledger as an evidentiary source	Attacks, reorganisations, inconsistent finality	Requirements for "jurisdictional finality"; independent audit
Smart contract	Automated execution of licence/royalty terms	Contractual constructs; digital self-governance	Code bugs; "code vs. intent of the parties"	Dual form: text + code; arbitration clauses; pause/upgrade mechanisms
Tokenization of rights (NFT/access tokens)	Marking/circulation of access rights	Virtual assets; licensing permissions	Confusion of "NFT ≠ copyright"	Standardized rights metadata; public clarification of legal scope (WIPO)
Provenance metadata	Source verification, good faith	Evidence, anti-plagiarism, rights management	Metadata forgery; Sybil identity attacks	Verified credentials; reputation protocols
Usage logging (access logs)	Accounting for royalty-relevant usage	Collective management; remuneration calculation	Privacy; excessive surveillance	Data minimisation; differential privacy; access control
Access management (permissioning)	Control of lawful use	Contractual regimes; technical protection measures	User discrimination; "lock-in"	Transparent rules; appeal mechanisms; algorithmic transparency
Interoperability (bridges, standards)	Mutual recognition of records/licences	Legal interoperability, cross-border conflicts	Different evidentiary standards; licence incompatibility	Unified evidentiary profiles; mutual-recognition policies
AML/KYC for rights marketplaces	Preventing abuse and money laundering	Financial compliance for content monetisation	Privacy risks; user exclusion	Risk-based KYC; proportionality; complaint procedures
Evidence storage (off-chain repositories)	Chain of custody, availability	Electronic evidence; procedural standards	Loss of access; substitution	Backup; integrity control; notarisation of digital facts

Table 13. Regulatory Models

(author's typology)

Model	What Exactly Is Regulated	Institutions / Mechanisms	Risks to Innovation	Risks to Human Rights
Techno-neutral	Copyright retains classical categories; technologies are merely "channels" and "carriers"	Court interpretation; general protection rules; special TDM/exception norms	Uncertainty for new protocols; "after-the-fact" enforcement	Risk of private censorship by platforms due to fear of liability
Financial-risk-based	Focus on content-monetisation markets (marketplaces, rights tokenisation, royalty payments)	AML/KYC, oversight, provider requirements, transaction transparency	High transaction costs; entry barriers for small creators	Excessive data collection; user exclusion; "deplatforming"
State-controlled	Registration regimes, real-name requirements, provider permits, content restrictions	Platform licensing; centralised registries; administrative sanctions	Slower innovation; migration of projects into the "shadows"	Disproportionate restrictions on freedom of expression and privacy

Table 14. Metaverse Objects: Characteristics and Status

(author's typology)

Metaverse Element (Entity)	Object of Protection / Rights	Key Obligations	Protocol Data for Evidentiary Purposes	Jurisdictional Implication
Avatar (as a digital persona)	Visual image, skin, voice, animations, scripts	Usage licences; prohibition of copying; moral rights	Asset hashes; creation/purchase logs; licensing tokens	Determining the lawful user; identifying the infringer
Digital twin	Models, data, synthesised media	Limits of use; prohibition of substitution; attribution	Provenance signatures; timestamps; access policies	Disputes over origin and substitution; need for due process
Virtual space (scene / world)	Composition, 3D scenes, music, interfaces	Complex licences for a composite work	Versioning; modification logs; co-creator rights	Delineation of contributions; collective management / DAO
User-generated content (UGC)	Derivative works, remixes, mashups	Defining fair-use limits; permissions	Source labelling; permission records	Automated disputes and appeals; proportionate sanctions
Marketplace / platform	Catalogs, metadata, moderation rules	Provider obligations; notice-and-action mechanism	Decision logs; algorithmic transparency	Review of procedural fairness; algorithmic transparency
AI content generator	Generation output; training data	Disclosure of AI involvement; copyright-compliance policy	Explainability; training summary; prompt logs (regime-dependent)	Legality review; audit; mutual recognition of evidence

Table 15. Summary Characteristics of the Survey Blocks

"Analysis of the Impact of AI Technologies on Ukrainian Society" — author's typology

No.	Question	n	Dominant Answer
1	What is artificial intelligence to you?	n/a	A tool of influence over people — 57%
2	Where are the most important technologies born?	96	Joint projects of science and business — 47%
3	Should AI be allowed to clone itself autonomously?	174	No, it could be dangerous — 60%
4	Who should be responsible for AI decisions?	94	The owner company / operator — 49%
5	Are you ready to entrust children's futures to AI algorithms?	61	Important decisions — only by a human — 72%
6	How often should you share photos/videos of your child on social media?	90	Never — 80%
7	Trust in AI recommendations (credit, treatment, education)?	374	Only as a suggestion — 61%
8	How do you perceive AI — a tool or a threat?	223	A tool / executor — 61%
Σ	Total (across all blocks)	1,112	2024–2025

Table 16. Characteristics of Clusters of Attitudes Toward AI Technologies

(author's typology)

Cluster	%	Characteristics
"Skeptics"	48	Reject AI autonomy; insist on human primacy; support strict regulation. Correlate with demand for EU AI Act-compatible legislation.
"Pragmatists"	38	Accept AI as a tool subject to operator control and transparency; support a strict-liability model for operators.
"Optimists"	14	Ready for extensive delegation of authority to AI; open to recognising AI as a legal subject; support science-business partnerships.

Table 17. Legal Risk Matrix of AI Based on Survey Results

(author's typology)

Topic	Concern Level	Regulation	Legal Norm
Trust in AI for critical decisions	High (94%)	Critical	EU AI Act Art. 14 (human oversight); GDPR Art. 22
Autonomous AI self-replication	High (60%)	Critical	EU AI Act Art. 5 (prohibited practices)
Operator liability	Medium (49%)	High	EU AI Act Art. 3 (deployer); strict-liability model
Children's privacy	High (80%)	High	GDPR Art. 8, 25; UNCRC General Comment No. 25 (2021)
AI legal personhood	Medium (13%)	Debated	EPRS 2017 ("electronic personhood"); EU AI Act — no consensus

Table 18. Legislative Recommendations for AI Regulation in Ukraine

(author's typology)

No.	Recommendation	Justification and Legal Basis
1	Establishing the human-in-the-loop principle	94% reject autonomous AI decisions in critical areas → Art. 14 EU AI Act; Art. 22 GDPR; implementation needed in the Law of Ukraine "On Personal Data Protection"
2	Operator liability for AI decisions	49% support an operator-liability model → Art. 3 EU AI Act (deployer); introduction of operator strict liability in the Civil Code of Ukraine / a special Law "On AI"
3	Protection of the "child's digital footprint"	80% "never" → GDPR Art. 8, 25; UNCRC General Comment No. 25 (2021); a special chapter in the Law "On Personal Data Protection"
4	Ban on autonomous AI self-replication	60% opposed → EU AI Act Art. 5 (prohibited practices); inclusion in the list of "unacceptable risk" systems in national legislation
5	Digital jurisdiction of the Metaverse	13% ready for AI legal personhood → development of a Digital Code of Ukraine regulating digital identity, avatars, and "delegated legal capacity" of AI in the Metaverse