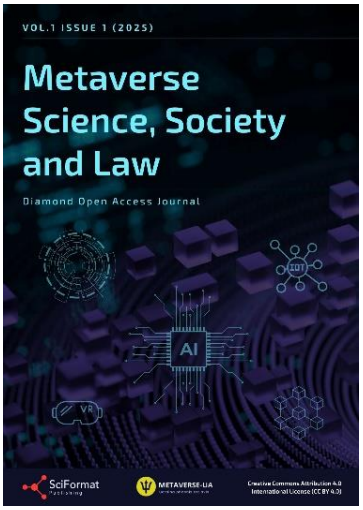

Metaverse Science, Society and Law

Vol. 1, Issue 1 (2025)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	RECONCEPTUALIZING JURISDICTION AND LEGAL IDENTITY IN THE METAVERSE: ELEMENTS OF A DIGITAL CODE ARCHITECTURE
ARTICLE INFO	Kostenko Oleksii, Zhuravlov Dmytro. (2025) Reconceptualizing Jurisdiction and Legal Identity in The Metaverse: Elements of a Digital Code Architecture. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.13
DOI	https://doi.org/10.69635/mssl.2025.1.1.13
RECEIVED	29 April 2025
ACCEPTED	22 June 2025
PUBLISHED	12 July 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

RECONCEPTUALIZING JURISDICTION AND LEGAL IDENTITY IN THE METAVERSE: ELEMENTS OF A DIGITAL CODE ARCHITECTURE

Kostenko Oleksii
Ph.D., State Scientific Institution «Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine», Ukraine. 3-A Askoldiv Alley, 01010 Kyiv; Ukraine
ORCID ID: 0000-0002-2131-0281

Zhuravlov Dmytro
D.Sc., Office of the President of Ukraine, Ukraine. Bankova 11, 01220 Kyiv; Ukraine
ORCID ID: 0000-0002-2205-6828

ABSTRACT

The rapid evolution of immersive technologies, decentralized platforms, and AI-driven systems within the Metaverse has exposed significant limitations in traditional legal regulation. This article proposes a modular Digital Code Model as a forward-looking legal framework designed to address the complexities of metaverse environments. Anchored in principles of semantic interoperability, algorithmic governance, and jurisdictional adaptability, the model introduces a layered legal architecture capable of responding dynamically to emerging digital phenomena. Key components include electronic jurisdiction, digital legal personality, AI-powered legal monitoring, and rights-based oversight mechanisms. Emphasizing the need for transnational coherence, machine-readability, and human-centric safeguards, the proposed model offers a scalable solution for regulating virtual spaces, ensuring legal predictability while preserving technological innovation and individual rights. The article outlines the theoretical foundations, structural modules, and implementation pathways of the Digital Code, positioning it as a foundational legal infrastructure for the governance of the Metaverse.

KEYWORDS

Digital Law, Digital Code, Metaverse, Artificial Intelligence, Digital Transformation, Legal Regulation

CITATION

Kostenko Oleksii, Zhuravlov Dmytro. (2025) Reconceptualizing Jurisdiction and Legal Identity in The Metaverse: Elements of a Digital Code Architecture. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.13

Introduction.

The problem of forming an information code or a special law on information and regulation of the Internet is not new in the world legal thought. It dates to the second half of the twentieth century, 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 the first foundational documents were the UNESCO Recommendations on the Information Society [1,2,3] and the WSIS (World Summit on the Information Society) Strategy [4] of the early 2000s.

In the scientific environment, the idea of an “information code” was actively discussed in Japan, France, Germany and the United States. For example, the French “Code de l'économie numérique” [5], which was partly a codification of rules in the field of digital commerce, electronic signatures and data protection, became one of the first examples of a national approach to digital law. In Germany, the reform of the Bundesdatenschutzgesetz [6], the Data Protection Act, had a significant impact, and it became the central legal mechanism for regulating information flows. In the United States, a sectoral approach was more common, with the Communications Decency Act [7], the Children's Online Privacy Protection Act [8], and 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, such as the Digital Services Act [9] , Digital Markets Act [10], and AI Act 2024, are quasi-codes that already contain a modular structure and elements of platform self-regulation, algorithmic control, and data interoperability.

In the scientific field, a thorough comparative legal study was conducted in the works of Lawrence Lessig "Code and Other Laws of Cyberspace" [11], who argued that the code and architecture of digital environments are already de facto law, and law should not only codify but also shape 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, but the draft of this legal act turned out to be cumbersome and full of terminology that is now outdated.

In the context of intense digital transformation, social and economic systems are undergoing profound structural shifts driven by the introduction of advanced technologies. Artificial intelligence, cloud computing, quantum solutions, and immersive environments such as the Metaverse are shaping a new configuration of digital reality, characterized by high complexity, interactivity, and dynamics [12].

In such circumstances, traditional legal constructs such as jurisdiction, legal personality, and regulation are showing significant limitations. Their effectiveness is declining against the backdrop of a globalized, decentralized, and fast-moving digital environment, to which classical legal instruments were not adapted. The current legal architecture, formed in the era of analogue relations, is less and less in line with the parameters of modern technological realities.

In response to these challenges, we propose the Digital Code Model, a new generation regulatory system designed to meet the needs of the digital age. A distinctive feature of the model is its functional flexibility and ability to be constantly updated, which is achieved through built-in legal monitoring algorithms based on artificial intelligence and the activities of interdisciplinary expert bodies.

This combination of tools allows for rapid adaptation of legal norms to changes in the technological and social context. As a result, the model contributes to improving the efficiency of legal regulation and ensures that the legal system is properly aligned 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 aims to strike a balance between innovative technological development, respect for fundamental human rights and preservation of the institutional security of the state in the globalized information space.

The development of this model is a response to several fundamental challenges faced by modern jurisprudence in the era of digital transformation, in particular:

1. Globalization 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 regulation and coordination mechanisms between national jurisdictions.
2. Emergence of new legal subjects and objects. Digital agents built based on 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 new phenomena in the legal system with the definition of their legal personality, limits of legal responsibility and legal status within digital legal relations.
3. Regulatory lag. Traditional lawmaking mechanisms based on hierarchical and procedurally burdened rulemaking models show inertia and inability to respond quickly to technological innovations. Such regulatory inertia complicates law enforcement and creates situations of legal uncertainty.
4. Fragmented regulatory framework. The lack of coherence between different sectoral and industry-specific acts regulating digital relations causes fragmentation of the legal space, legal conflicts and a decrease in the effectiveness of legal influence. In response, the Model Digital Code envisages 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 formalize mechanisms for dynamic updating of the regulatory framework. The model's architecture includes several key components: algorithmic monitoring of legal changes, expert advisory mechanisms involving interdisciplinary expertise, and legal audit systems integrated with digital registries and the open data infrastructure.

Special attention is paid to the artificial intelligence module, which serves as the analytical core of the system. Its task is to continuously analyze the technological context, social transformations, and changes in international law to promptly update regulatory provisions. The model envisages an open roadmap for implementation based on the principles of gradual harmonization with national legal systems and international standards.

Thus, the Digital Code Model serves as a conceptual foundation for building a new digital law architecture that is adaptive, transparent, and future-oriented. Its implementation will help eliminate a few 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.

Theoretical foundations of the Digital Code Model in the context of digital transformation

The evolution of legal systems reflects the dynamics of social change. In the industrial era, codes, such as the Napoleonic Code, were created to regulate stable and localized social relations. However, with the advent of the digital era, marked by the concept of Society 5.0, which envisages the harmonious integration of technology and human activity, a new legal paradigm has emerged. Information law, as an independent field, focuses on the regulation of digital interactions, data flows, and new legal entities such as artificial intelligence agents and decentralized autonomous organizations (DAOs).

Digital transformation poses several 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 emphasize the need to create adaptive legal systems that can evolve along with technology while maintaining stability and predictability of legal regulation. The proposed Digital Code Model is 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 International Organization for Standardization (ISO) standards - to ensure global compatibility and efficiency.

The formation of the Digital Code Model involves several successive stages, each of which performs a specific methodological function (fig.1):

1. Doctrinal analysis of the regulatory framework. At this stage, an in-depth systematic study of the existing array of legal acts in the field of information and digital law is carried out. The aim is to identify regulatory gaps, logical and semantic contradictions, and to identify the rules that have lost their effectiveness in the context of new technological realities. Special attention is paid to institutional conflicts between sectoral regulations and supranational law.
2. 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 solutions to the local legal mentality and regulatory context.
3. Legal design and machine-readable structure. This stage involves the engineering design of the model as a digital legal environment. The emphasis is on modularity, which ensures that the system is built from separate logically complete components (legal domains, registration modules, access interfaces), as well as on machine readability, which is the ability of legal norms to be interpreted by computer systems. This, in turn, ensures 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. This approach makes the Digital Code Model capable of continuous evolution in line with changes in the socio-technical environment, as well as integration into the international regulatory ecosystem through compliance with ISO, W3C, IEEE standards and the UN institutional framework on digital rights and sustainable development.

As a result, the chosen methodology allows for the design of 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 information society.

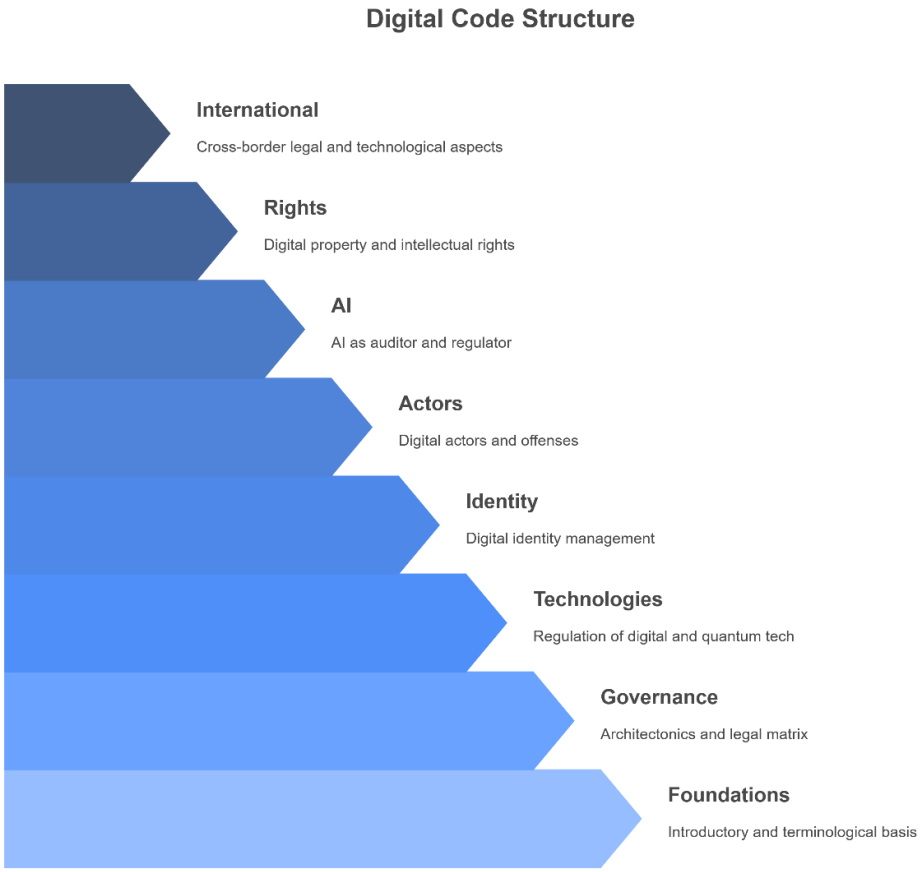

Fig. 1. *Digital Code Structure*

The general topology of the Digital Code Model may consist of various modules that will structurally and systematically contain the regulatory functions of any sphere of human activity related to and created with the use of modern information and immersive technologies. Let us consider only the basic modules that, in our opinion, will form the foundation of the Digital Code, namely:

Module I. Introduction

Module I provides a conceptual framework justifying the creation of a new legal system capable of meeting the challenges of the digital age. It explains the limitations of traditional codes that are unable to cover new forms of legal relations arising from autonomous agents, global digital flows, cryptocurrency assets, Metaverse interfaces and virtual entities. The author points out the key problem, namely regulatory lag, which makes it impossible to respond in a timely manner to technological changes.

This approach envisages a modular structure that combines the stability of principles with the ability to be updated quickly. 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 that law cannot only react but also proactively shape the regulatory environment, including new categories of legal personality and forms of digital ownership.

The module also emphasizes the global dimension of digital processes and, accordingly, the need for interjurisdictional harmonization. It emphasizes the need to harmonize legal regimes in the transnational digital environment. The proposed model complies with international standards and is designed to meet the requirements of global interoperability.

It is intended to lay the foundations for transnational legal interoperability by integrating international digital standards, such as the Digital Services Act, ISO/IEC, OECD Digital Governance Recommendations.

Thus, the Introduction serves as the theoretical and strategic foundation of the entire model, forming the starting point for the formalization of digital law in the context of technological turbulence and the era of post-industrial legal architecture.

Module II. Terminological and methodological framework

The basis of Module II is defined by the semantic framework of the model by creating a dynamic, machine-readable and updated glossary of digital legal terms. This glossary is not only a reference tool, but also a foundational element supporting other modules, including norms repositories, digital solutions, smart contracts, and interoperable services.

The terminology is developed considering 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 representing national jurisdictions and cross-border electronic jurisdiction: lawyers, technologists, linguists and information modeling experts.

The module is methodologically based on the concept of legal design and the principles of semantic interoperability. This allows for unambiguous interpretation of terms by both human and machine intelligence, as well as integration with governmental and supranational digital governance systems.

As a result, Module II ensures the semantic integrity, logical consistency, and technical adaptability of the entire body of legal provisions of the Digital Code.

Module III. Core principles

Module III sets out the basic principles of digital law that form an integral part of the Digital Code's architecture. They serve as a regulatory "framework" that guides the development of all subsequent regulatory provisions and practices. The key principles include technology neutrality, digital inclusion, human rights, algorithmic responsibility, data security, and algorithmic transparency.

These principles set moral and legal boundaries for digital governance, preventing technocentrism and regulatory relativism. Particular attention is paid to ensuring a balance between innovation and legal safeguards; for example, between automated decision-making and the individual's right to appeal [13].

The module also emphasizes the priority of the human being as the central subject of the digital society: technologies should serve rights, freedoms and dignity, and not vice versa. Such an anthropocentric vector allows preservation of the humanistic identity of law even within high-tech environments. At the same time, provisions are being introduced that provide for the possibility of granting rights, duties and responsibilities to a specific class of digital entities and agents.

Ultimately, 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 lawmaking.

Module IV. Repository of current regulations

The creation of a centralized digital repository of current regulations governing digital processes is envisaged under Module IV. The repository performs the functions of storing, cataloguing, updating, and automatically detecting outdated or conflicting regulations. It is based on a semantic model of legislation supported by artificial intelligence and machine analysis.

The repository allows integration of both national and international acts, ensuring their interoperability and adaptation to the local context. In addition, it supports the function of comparative law function - the ability to compare similar rules in different jurisdictions to harmonize digital regulation.

The process of updating the regulatory array is carried out both automatically (using update algorithms) and manually - through an audit conducted by an expert council. This approach ensures that the legislation is always up-to-date and that regulatory gaps requiring lawmaking are identified in a timely manner. The repository serves as the basis for the functioning of all digital regulation modules and acts as a guarantor of regulatory consistency.

Module V. Digital governance architecture

This module defines the organizational and functional model of digital governance as a component of the institutional structure of the Digital Code Model. It outlines the construction of a multi-level architecture within which government agencies, digital regulators, scientific and expert councils, and AI modules for regulatory analysis interact with each other.

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 lawmaking, smart contracts for administrative decisions, and digital platforms for real-time public consultations.

The module also includes provisions on transparency of governance, electronic document management, real-time monitoring and cross-sectoral coordination in the digital environment. Interaction with international governance institutions and support for regulatory compatibility with the digital policies of the EU, OECD, ITU and other global structures are ensured.

The architecture of digital governance outlined in the module creates the basis for an effective, open and flexible regulatory environment that is consistent with the principles of democracy, innovation and technological responsibility.

Module VI. Legal and systemic framework for digital communication

The regulatory framework for the functioning of the digital communications infrastructure, including Internet protocols, telecommunications platforms, satellite communications, data exchange systems and next-generation (5G and beyond) architectures, is set out in Module VI. The module ensures the integrity of the legal regulation of information exchange in decentralized and cross-border networks.

The main areas of regulation include: spectrum management, technical standards and interfaces, operator licensing, user rights protection, protection of critical information infrastructure, and ensuring non-discriminatory access to digital communications.

The module envisages 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 planned to create a mechanism for attributing digital 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 digital service providers.

Module VII. Electronic jurisdiction

Module VII develops the legal doctrine of jurisdiction in the digital space, considering new forms of cross-border interaction, the lack of physical localization of servers and the specifics of the activities of digital entities. It departs from the classical territorial approaches, offering functional, network and algorithmic models of jurisdiction.

It introduces the concepts of digital presence, data storage, transaction coding (code of actions) and verification of participants using cryptographic methods. The module defines the criteria for jurisdictional linkage in smart contract systems, decentralized platforms, Metaverse environments, and blockchain infrastructures [14].

The module also regulates the procedure for the recognition of electronic evidence, digital transactions, and liability of participants in a multijurisdictional environment. It provides for mechanisms for mutual delegation of jurisdiction between national systems and the establishment of supranational digital arbitration.

E-jurisdiction is a key tool for ensuring legal certainty in transnational digital processes, allowing one to establish a link between the subject, the digital environment and the applicable law in a complex information landscape.

Module VIII. Legal digital technologies regulation

The module establishes the legal framework for the development, implementation and control of modern digital technologies - artificial intelligence, the Internet of Things (IoT), blockchain systems, neural networks, big data, cloud platforms and automated interfaces.

The central task is to strike a balance between stimulating innovation and preventive legal control. Requirements are being introduced to ensure transparency of algorithms, explainability of decisions, a risk-based approach to the classification of technologies, and the principle of developer and operator responsibility.

Particular attention is paid to the observance of ethical standards and human rights in automation processes, including non-discrimination, protection of privacy, and the right to refuse machine interference. The module provides mechanisms for certification of digital systems, licensing of critical technologies, and regulatory modelling of pilot projects.

This approach is based on the principles of techno-ethical legitimacy, dynamic legal support of the innovation cycle, and integration with global digital regulatory initiatives, including the EU AI Act, IEEE Ethically Aligned Design, and UNESCO's recommendations on AI ethics.

Module IX. Legal regulation of quantum technologies

This module defines the legal framework for the use, development and application 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 representing actions within 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 non-transparent quantum systems, and the role of the state in ensuring technological sovereignty through the creation of quantum hubs.

On the legal level, 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

Module X establishes the regulatory framework for the functioning of digital identification systems within a virtualized legal environment. It covers the legal regulation of personal identifiers (digital profile, biometric and behavioural markers), authentication, verification and access control mechanisms [15].

The concept of digital identity is introduced as a multi-level legal construct that includes decentralized elements, blockchain records, zero-knowledge proofs, and digital subscriptions. The principles of data minimization, 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 contains mechanisms for liability for compromise or unauthorized 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

Module XI focuses on regulatory framework for the development of immersive 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 agents 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.

Module XI is key to shaping the concept of "virtual ethics", protecting personal data in deeply interactive environments, and developing legislation that regulates the hybrid reality of physical, digital and emotional-cognitive dimensions.

Module XII. Legal regulation of the Metaverse

Module XII establishes a regulatory model for governing the Metaverse as interactive virtual environments powered by immersive technologies, blockchain infrastructures, and artificial intelligence algorithms. The goal is to form a legal framework for activities in decentralized virtual spaces [16].

The concepts of digital territoriality, tokenized jurisdiction, virtual citizenship, and contract reality are 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 authentication of actions, recording of transactions, conflict resolution, and content moderation. 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 [17].

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 [18], autonomous organizations (DAOs), robotic systems, and virtual representations. Its purpose is to formalize 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 oversight).

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.

Module XIV. Digital offenses and punishments

The module systematizes the categories of offenses 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 (unauthorized access, malware, data manipulation) and the latest violations related to autonomous systems, algorithms and virtual environments [19].

The concepts of algorithmic guilt, digital intent, and machine negligence are introduced. A system of punishments is established, considering both the legal nature of the subject (human, AI, DAO) and the level of risk, the degree of public danger and autonomy of actions [20].

Particular attention is paid to the regulation of digital evidence, attribution of offenses, jurisdictional cooperation, as well as the implementation of the principle of digital justice. The functions of digital prosecutorial entities, 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 [21], revision and interpretation of legal norms [22]. 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 legal database, is introduced [23]. AI carries out thematic structuring, time verification, classification by level of relevance and risk analysis of possible regulatory gaps [24].

The results of AI monitoring are presented in the form of reports, analytical dashboards and recommendations for law-making and control bodies. A restriction on the autonomous intervention of AI in law enforcement has been determined — it is allowed only accompanied by a human curator.

As a result, the module forms a regulatory architecture of built-in digital self-control, ensuring the stability, relevance and accountability of the legal system in a highly dynamic digital environment.

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 conducts primary analysis, forms draft proposals for legislation updates, and models scenarios of legal impact.

The regulator acts within the conditions of normatively defined boundaries and according to clearly prescribed procedures: all recommendations are validated by 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 transparent 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 works in the virtual environment. It covers tokenized assets (NFTs), digital works, artificially generated content, software, data, algorithms, and digital things[25].

The concept of "digital thing" is introduced as an independent object of civil circulation, which is subject to the legal regime of ownership, use and disposal. The methods of confirming ownership through blockchain registers, digital signatures, cryptographic protocols and quantum tokens are determined [26, 27].

In the field of intellectual property, the module regulates the creation, licensing, transfer, and protection of rights to objects generated with the involvement of AI [28]. 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, equitable 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.

Module XVIII. Cyber diplomacy

The module develops the conceptual and normative foundations of cyber diplomacy as a tool of the state's foreign policy in the digital environment. Cyber diplomacy [29] is considered a system of multi-level legal and technopolitical measures aimed at resolving cross-border incidents, coordinating international law-making and ensuring digital sovereignty [30,31].

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 [32,33].

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, scope of authority 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 digitalization.

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 [34].

The sandbox functions as a limited digital environment with modified norms [35], within which entities can implement experimental products: AI platforms, blockchain infrastructures, quantum services, digital currencies, virtual jurisdictions, Smart Law protocols [36].

Mechanisms for preliminary risk assessment, temporary authorization, supervisory expertise and provisional liability are being introduced [37]. Sandbox participants operate under the control of a digital supervisory board and have the obligation to publicly report on the results of the experiment.

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 creating a cross-border digital court as a dispute resolution tool in a multi-jurisdictional digital environment [38, 39]. The court operates based on cloud infrastructure, smart contracts, and virtual presence technologies.

The court will specialize 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 visualisation 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 regulatory environment 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 [40].

Its instruments include expert audits of digital policies, real-time analysis of regulatory data, conducting cloud inspections, providing advice to governments and developers [41]. Activities are coordinated with the structures of the UN, EU, Council of Europe, WIPO **(**WIPO), ISO [43].

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.

Module XXII. International Scientific Expert Council on Digital Technologies, Ethics and Law

Module XXII defines the regulatory and organizational 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, specialists in digital ethics, technology lawyers, developers and analysts from different countries [43]. The main functions are preparation of international standards of digital behaviour, assessment of legal risks of the latest technologies, advising international organizations and states on the observance of human rights in the digital sphere [44].

The module also provides for the development of a Code of Ethics for Digital Civilization, the Council's participation in the implementation of global initiatives on responsible AI, digital security ecosystems, eco-digital balance, as well as the development of academic platforms for legal foresight.

Thus, the International Council is becoming a key analytical-prognostic and normative-ethical actor that ensures a civilizational 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 revisions of norms, terminology, and interoperability formats through integrated AI monitoring — without affecting the content core of the Code [45]. Structural changes include the reorganization 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 overall concept and paradigm of the Code.

The change procedure is based on an automated system for processing initiatives, which includes AI-monitoring of the regulatory environment; semantic classification of changes (according to criteria G1-G5); formalization of proposals in the Smart Norm Draft format; digital expertise by an AI regulator; verification by the National Expert Council; public discussion; formal approval (automatic or parliamentary).

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–XXIIII 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, considering 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 integration.

It is envisaged to create an International Synchronization Platform (Digital Norm Sync 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 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.

Conclusions

The digital transformation of society, which covers all spheres of human existence — from communication to legal regulation — requires a radical rethinking of the forms and mechanisms of creating, applying and updating legal norms. 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 machinability and ethical and legal responsibility.

The structure of the Code, organized according to the modular principle, allows you to synchronize 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 considers 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 civilization. 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.

Commentary.

The original article is indexed in the Creative Commons Attribution (CC BY) 4.0 system and available at: Kostenko Oleksii, Zhuravlov Dmytro. (2025). METAVERSE: THE DIGITAL LAW OF THE DIGITAL AGE. In Kostenko Oleksii, Kharytonova Olena, & Kharytonov Yevhen (Eds.), DIGITALIZATION, METAVERSE, ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF HUMAN AND INDIVIDUAL RIGHTS PROTECTION IN UKRAINE AND THE WORLD (pp. 5-20). SciFormat Publishing Books. https://doi.org/10.69635/978-1-0690482-4-0-ch1

REFERENCES

1. Aristova, I. V. (2009). Organizational and legal mechanisms of UNESCO for the development of the information society – a guidepost for Ukraine. *Information and Law*, 1(21), 19-23. Available at: https://ippi.org.ua/aristova-iv-organizatsiino-pravovi-mekhanizmi-yunesko-shchodo-rozvitku-informatsiinogo-suspilstva-%E2%80%93
2. UNESCO. (2024). Constitution of the United Nations Educational, Scientific and Cultural Organization (adopted on 16 November 1945). Available at: https://www.unesco.org/en/legal-affairs/constitution?hub=66535
3. World Summit on the Information Society Geneva 2003 – Tunis 2005 (WSIS). Declaration of Principles: Building the Information Society: a global challenge in the new Millennium (WSIS-03/GENEVA/Doc/4-R). *International Telecommunication Union*. Available at: https://www.itu.int/net/wsis/docs/geneva/official/dop.html.
4. World Summit on the Information Society Geneva 2003 – Tunis 2005 (WSIS). Available at: https://www.itu.int/net/wsis/
5. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1). Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/2021-07-26/
6. Bundesdatenschutzgesetz (BDSG). Available at: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html.
7. 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. Available at: https://www.law.cornell.edu/uscode/text/47/230
8. Federal Trade Commission. (FTC). Protection American Consumers. Children's Online Privacy Protection Act. Available at: https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act
9. 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) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
10. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng
11. Lessig, L. Code and Other Laws of Cyberspace. Basic Books, Inc. New York, 1999. ISBN-13: 978-0-465-03912-8.
12. Kostenko, O., & Yekhanurov, Y. (Eds.). (2024). *Digital transformation in Ukraine: AI, Metaverse, and Society 5.0.* SciFormat Publishing Books. DOI: https://doi.org/10.69635/978-1-0690482-1-9.
13. 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. DOI: https://doi.org/10.22598/iele.2023.10.1.10.
14. 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.
15. Kostenko, O. V., Mangora, V. V. (2022). Directions of legal regulation development of identity data management. Information and Law, 1(40), 54-60. DOI: https://doi.org/10.37750/2616-6798.2022.1(40).254342.
16. Kostenko, O. V., Golovko, O. M. (2023). Electronic Jurisdiction of the Metaverse: Challenges and Risks of Legal Regulation of Virtual Reality. Information and law, 1(44), 105-115. Available at: http://ippi.org.ua/kostenko-ov-golovko-om-elektronna-yurisdiktsiya-metaverse-vikliki-ta-riziki-pravovogo-regulyuvannya
17. Kostenko, O. V. (2022). 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.
18. Kostenko, O. V., Mangora, V. V. (2022). Metaverse: Legal prospects of regulation application of avatars and artificial intelligence. *Legal Scientific Electronic Journal*, (2), 102-105. https://doi.org/10.32782/2524-0374/2022-2/23.
19. 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.
20. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border Criminal Investigations and Digital Evidence. *ArXiv*, abs/2205.12911. Available at: https://doi.org/10.48550/arXiv.2205.12911.
21. Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices. *Administrative Sciences*. https://doi.org/10.3390/admsci14100238.

22. 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.
23. Hanfy, F., Alakkas, A., & Alhumoudi, H. (2024). Analyzing the role of digitalization and its impact on auditing. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-19729-0.
24. Rao, N. (2024). Audit Through Artificial Intelligence Tools. *The Management Accountant Journal*. 59(10), 61-62. DOI: https://doi.org/10.33516/maj.v59i10.61-62p.
25. Foster, C. (2023). Intellectual property rights and control in the digital economy: Examining the expansion of M-Pesa. *Information Society*, 40(1), 1-17. https://doi.org/10.1080/01972243.2023.2259895.
26. Sreeganesh, U. (2024). Role of Intellectual Property Rights in Digital Era. *International Journal of Judicial Science Research Studies (IJJSRS)*, 1(1), 22-26. DOI: https://doi.org/10.5281/zenodo.13986696.
27. 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. DOI: https://doi.org/10.36719/2706-6185/04/49-51.
28. Baiurchak, M., Kiriiak, O. (2024). Intellectual property rights within the digitization. *Digitalization of legal deeds in the context of the modernization of public services 2022*, 93-98. https://doi.org/10.59295/daj2022.13.
29. Banihashemi, S. S. A. (2021). Cyber Diplomacy. *Cyber Diplomacy*, 1-106. https://doi.org/10.9734/bpi/mono/978-93-91473-74-7.
30. 30 Tsaugourias, N.(2018). Law, Borders and the Territorialisation of Cyberspace. Indonesian Journal of International Law, 15(4), 523-551. DOI: https://doi.org/10.17304/ijil.vol15.4.738.
31. 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.
32. Kostenko, O. V., Zhuravlov, D. V., Nikitin, V. V., Manhora, V. V., Manhora, T. V. (2024). A Typical Cross-Border Metaverse Model as a Counteraction to Its Fragmentation. *Bratislava Law Review,* 8(2), 163-176. https://doi.org/10.46282/blr.2024.8.2.844.
33. 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.
34. Kostenko, O. V., Volkova, Y. A., Ustynova, I. P., Shapenko, L. O., & Usenko, Y. V. (2024). Legal perspectives of the International Scientific Sandbox Metaverse: Technologies and foresights for digital transformation. *Advanced Metaverse Wireless Communication Systems* (Chap. 18), 519-548. https://doi.org/10.1049/PBTE112E_ch18.
35. 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.
36. Tsai, C. H., Lin, C. F., & Liu, H. W. (2019). The Diffusion of the Sandbox Approach to Disruptive Innovation and Its Limitations. *Cornell International Law Journal*, 2020, 53(2), 1-37. Available at: http://dx.doi.org/10.2139/ssrn.3487175.
37. 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.2023.113656.
38. 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.
39. 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.
40. 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. *J. Theor. Appl. Electron. Commer. Res.*, 18, 777-794. https://doi.org/10.3390/jtaer18020040.
41. Zhu, L., Yang, L., Li, C., Hu, S., Liu, L., & Yin, B. (2024). LegiLM: A Fine-Tuned Legal Language Model for Data Compliance. *ArXiv*, abs/2409.13721. https://doi.org/10.48550/arXiv.2409.13721.
42. Burk, D. (2005). Legal and Technical Standards in Digital Rights Management Technology. *Fordham Law Review*, 74, 537-573. https://doi.org/10.2139/SSRN.699384.
43. Mahieu, R., Van Eck, N., Van Putten, D., & Van Den Hoven, J. (2018). From dignity to security protocols: a scientometric analysis of digital ethics. *Ethics and Information Technology*, 20, 175-187. https://doi.org/10.1007/s10676-018-9457-5.
44. Rochel, J. (2023). Error 404: looking for trust in international law on digital technologies. *Law, Innovation and Technology*, 15, 148-184. https://doi.org/10.1080/17579961.2023.2184139.
45. Sattlegger, A. (2024). Ethical Governance of Emerging Digital Technologies in the Public Sector - Insights from Dutch Digital Ethics Commissions, 131-146. https://doi.org/10.1007/978-3-031-70804-6_9.