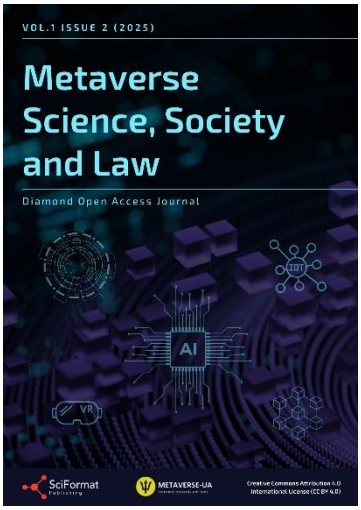

Metaverse Science, Society and Law

Vol. 1, Issue 2 (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	DIGITAL JURISDICTION
DOI	https://doi.org/10.69635/mssl.2025.1.2.23
RECEIVED	26 July 2025
ACCEPTED	06 October 2025
PUBLISHED	17 October 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

DIGITAL JURISDICTION

Kostenko Oleksii
Ph.D., Associate Professor, State Scientific Institution «Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine», Ukraine.
ORCID ID: 0000-0002-2131-0281

ABSTRACT

The scientific work is a logical continuation of the author's many years of research devoted to the formation of the paradigm of digital jurisdiction — a new legal system for the digital and immersive environment of the Metaverse. If previous works outlined the conceptual foundations of this phenomenon, the current study for the first time structures digital jurisdiction in the format of a holistic model that combines the technical, ethical, procedural and legal levels of digital governance. The model is considered as a normative architecture of the future — a kind of "metaoperating system" for regulating social relations in virtual spaces, which transforms the classical principles of sovereignty, jurisdiction and responsibility in the online world.

The article offers a methodological scheme for building an digital jurisdiction based on a modular approach, which allows it to be integrated into the system of national and international law. Particular attention is paid to institutional and procedural components — digital courts, ombudsmen, cross-border arbitration, as well as the principles of algorithmic legitimacy and ethical-centric governance. Digital jurisdiction is interpreted as a tool for civilizational adaptation of law to the age of Web 4.0, blockchain legal protocols and artificial intelligence.

This study not only systematizes the established theory but also offers a conceptual shift from the declarative level to modelling the operational legal system of the future, opening prospects for the creation of digital codes, registers and international regulatory platforms. The author encourages the scientific community to a deep discussion about borders, subjectivity, and justice in digital civilization, because digital jurisdiction is not just a new legal form — it is a matrix for restarting law and order in post-physical reality.

KEYWORDS

Electronic Jurisdiction, Digital Jurisdiction, Metaverse, Digital Law, Algorithmic Governance, Artificial Intelligence, Digital State, Digital Code, AI, Metaverse, Digital Sovereignty, Law, Web 3.0, Digital Identity, Blockchain, Avatar

CITATION

Kostenko Oleksii. (2025) Digital Jurisdiction. *Metaverse Science, Society and Law*. Vol. 1, Issue 2. doi: 10.69635/mssl.2025.1.2.23

Introduction.

The history of human civilization demonstrates the consistent evolution of communication forms that determined the structure of social interaction and knowledge transfer. The first was the verbal era, in which information was transmitted exclusively orally, and the preservation of knowledge was ensured by the memory of generations. The second, the verbal-sign era, was characterized by the emergence of symbols, gestures and primary writing systems, which made it possible to fix meaning and expand the space of communication. The next, verbal-written epoch associated with the emergence of writing and printing, laid the foundation for the mass dissemination of knowledge and the formation of institutions of science, education and law.

Today, humanity has entered the fourth era — the age of electronic communication, in which digital technologies not only combine, but also transform all previous forms of information exchange. From the first computers to global networks, from isolated systems to integrated platforms, this era creates a new quality of social interaction based on the integration of artificial intelligence, the Internet of Things, and virtual environments.

In this context, the Metaverse appears as not just a new communication phenomenon, but as a complex sociotechnological system — a kind of constructor of modern civilization. It acts as an accumulator of

technological progress, a platform for the integration of man and machine, a space for creating new forms of interaction and self-realization. philosophical and legal understanding. Metaverse is understood as 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 enable their interaction [1].

1. Code as the Constitution of Cyberspace: From Lessig to the Architecture of Electronic Jurisdiction

Modern analog law, built on territoriality, physical borders and state control, is increasingly incapable of regulating social relations in digital ecosystems. These ecosystems — from decentralized networks to the Metaverse — operate on principles that have no spatial or national ties. In the Metaverse, people, avatars, digital twins, and autonomous artificial actors interact, and exchange occurs through codes, algorithms, and data, rather than through physical institutions or borders. Such cross-border digital spaces form 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 — electronic jurisdiction, which is designed to respond to the challenges of the digital age. Currently, this approach has no analogues. That is why the proposed Metaverse Model of Digital jurisdiction should become the basis not only for scientific discussions, but also for legal research aimed at creating primary model legislative acts. These acts should ensure the legal regulation of public relations in the Metaverse and initiate the digital transformation of analog regulatory documents.

The foundation of digital jurisdiction is the "Declaration of Independence of Cyberspace" by J. P. Barlow [2], as well as "Code and Other Laws of Cyberspace" and "Code" by L. Lessig [3, 4].

According to Lawrence Lessig, the architecture of cyberspace — that is, its technical structure, functionality, and program code — is the main regulator of the digital environment. It is the code that determines the ways, boundaries, and order of user interaction in cyberspace, just as in the physical world, social relations are governed 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 for access to digital environments, determines the boundaries of privacy, security, freedom of action of users and forms algorithmic control regimes. Therefore, the program code acquires a normative significance — it is not just a technical tool, but a regulatory structure that determines what is allowed and what is prohibited in the virtual space.

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. This concept of L. Lessig opened a new stage in understanding the relationship between technology and law, initiating the direction of research, which now forms the foundations of the architectonics of electronic jurisdiction.

2. Problems of legal regulation of social relations in the Metaverse

The difference between the modern cyberspace Web 2.0 and Metaverse Web 3.0-4.0 is a change in the very nature of legal relations. In the Web 2.0 system, most 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.

That is why the processes of modeling, forecasting, and legal registration of new social relations in the Metaverse are of particular importance. They are aimed at determining their content, orientation and legal status — that is, at creating the basis for the formation of adequate mechanisms for their regulation. The key issues remain:

1. what meaning should be put into the concepts *of "social relations in the Metaverse"* and *"relations in the Metaverse"*;
2. under what conditions electronic subjects and objects can be endowed with rights inherent in a person;
3. what forms of justice can be applied in a virtual environment;
4. what responsibility will electronic subjects and objects endowed with human rights have.

Today, digital identities, avatars, and electronic humanoids can realistically reproduce the appearance, voice, and behavior of a person, both imaginary and real. Such duplication ceases to be exclusively a medical or scientific technology and requires strict control over the circulation of human identification data, particularly those belonging to the "red group" according to the author's classification or to the category of *sensitive personal data* in accordance with the GDPR.

Virtual assets — NFTs, smart contracts, tokens, virtual lands (Decentraland, The Sandbox) — are already real objects of digital law with which legally significant actions are taken. However, the rules of conduct in the Metaverse are currently formed mainly by technical copying of the legal norms of the physical

world and are of a corporate and contractual nature. At the same time, there is a tendency to transplant the norms of public morality into the Metaverse through the creation of cosmopolitan e-social relations without the established attributes of e-statehood or its own management system.

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 considering 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 modernize 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 as an offense 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 effect.

Despite this, Metaverse technologies are already giving rise to new types of legal relations that require regulation. They form not only new objects, but also special forms of subjectivity — artificial, symbiotic or hybrid. However, at present, such properties are set by developers and remain artificially designed, not legally defined.

Therefore, electronic law is virtually absent in the Metaverse, and its functions are partially performed by fragments of national legal systems. Traditional analog law adapts to digital realities extremely slowly, not keeping up with the dynamics of technological evolution. That is why the task arises to create a systemic legal framework for the Metaverse, which will ensure the coordinated coexistence of a person, technology and algorithm within a single digital legal order [5].

4. Legal entropy: degradation of classical pillars of law in digital ecosystems

Total digitalization 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 centralized 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. A regulatory lag arises: the rule-making cycle of states is years; while the digital protocol cycle is weeks [6].

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 [7].

E-ecosystems and the Metaverse are inherently cross-border and international, as they are organized 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-fulfillment 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, tokenized rights, access licenses);
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 protocol as a special form of lex special is for smart contracts and consensus mechanisms.

5. The End of the Peace of Westphalia: Law in the Age of Protocols and Platforms

The Westphalian paradigm proceeded from the principles of territorial integrity and the state's monopoly on law and coercion [8]. In the digital age, it is degraded due to the blurring of borders by data flows; the emergence of parallel legal orders (platforms, protocols, private standards); the asymmetry of capabilities between states and transnational technological networks. (cyber sovereignty) on the grounds of data localization, 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 localization, sovereign clouds); jurisdictional manoeuvring (selection of favourable regimes for protocols); Splinternet (incompatible technical and legal standards) proxy sovereignty of platforms (community rules and terms of service that 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, 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.

6. Formation of the infrastructure of digital civilization

The large-scale transformation of the global system into a digital one is characterized by tokenization, the ISO 20022 standard, AI and the formation of global digital hubs. The system of global asset circulation is moving to tokenization: real assets (RWA), obligations and access rights take on a programmatic form. Cryptocurrencies, stablecoins, and CBDCs provide instant settlement and programmability of payments. The ISO 20022 standard unifies the format of financial messages and becomes the "language" of interaction between banks, blockchains and payment networks. Blockchain provides immutability and transparency, AI provides adaptability and predictability, and the Metaverse provides a new plane of economic activity, labour, and consumption.

At the same time, digital hubs are being formed — countries and regions that combine computing power, data energy, and legal regimes: the United States — the core of fundamental AI models, cloud ecosystems, and venture capital; The United Arab Emirates and Saudi Arabia — large-scale data centres, dedicated data economic zones, and investments in AI and semiconductors; The European Union and the United Kingdom are regulatory centres for the ethics and security of AI, digital markets and data; Singapore, Switzerland, and Hong Kong — Web 3.0 and tokenization financial hubs; China — integration of industrial IoT, robotics, AI, and national digital currency.

Additional transformation drivers: Confidential Computing (TEE/SGX), Multilateral Computing (MPC), Zero-Knowledge (ZK), Quantum Resilience of Cryptography, 5G/6G and edge-computing (Distributed Processing), Satellite Networks (Global Connectivity), Cyber-Physical Systems (Robotics, Autonomous Vehicles), Unified Identity (DID/VC), Decentralized Autonomous Organizations (DAOs) as institutional innovators. Together, they form a digital macrocycle in which the legal order must be versioned, interoperable, and ethicocentric.

In this context, digital jurisdiction acts as Meta-Legal OS: human rights — as an unchanging "constitutional core"; identity, evidence, calculation and responsibility modules — functioning as updated legal packages; interstate protocols — as APIs of sovereignties that ensure interoperability and arbitration.

7. *Digital Jurisdiction*

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 formulate the basic author's definition: "*Digital jurisdiction is a post-territorial legal structure 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*."

In a conceptual sense, digital jurisdiction is an extended form of electronic jurisdiction. If *electronic* defines the technological basis — electronic documents, transactions, infrastructure — then *digital*

encompasses the full lifecycle of data, algorithms, rights, and ethical norms, including autonomous artificial systems, decentralized organizations (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 place 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 electronic 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 electronic courts, digital arbitrations, online notaries, registers of electronic decisions, automated evidence verification systems, and legal monitoring services. They operate based on 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:

1. legal relationships arising within digital platforms, blockchain networks, Metaverses, decentralized autonomous organizations (DAOs), virtual offices, government portals, smart ecosystems, digital exchanges, educational and communication environments, including immersive platforms that enable interaction between humans and artificial agents;
2. electronic transactions, administrative procedures, judicial proceedings, certification, licensing, registration, electronic notarization, digital transactions and other legally significant actions carried out in a virtual environment and generating legal consequences in a digital or mixed format;
3. electronic evidence, digital identity, smart contracts, decentralized 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.

8. Principles of functioning of electronic jurisdiction

The principles of functioning of digital jurisdiction include:

The principle of extraterritoriality. The effect of 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 [9]; if such an event creates legal consequences, affects the rights, duties or interests of persons in the legal field of the state, it is subject to national legislation [10]. This principle ensures that the state can protect its citizens, digital residents, and institutions in global cyberspace by overcoming the limitations of physical territory [11, 12]. It forms the basis for the legal recognition of cross-border actions in blockchain networks, Metaverses [13] 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 [14, 15].

The principle of legal identity. Each participant in electronic legal relations has a confirmed digital identity [16], which is recognized as equivalent to personal presence and ensures its legal status in all forms of digital interaction [17, 18]. 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 [19]. It has legal force for concluding contracts, participating in court procedures, submitting applications and receiving administrative services [20, 21]. Legal identity acts as the foundation of e-citizenship, allows you to establish responsibility for actions in cyberspace, prevents fraud and ensures verification of the legitimacy of digital transactions [22, 23]. Its presence is a prerequisite for the legitimacy of any actions within the digital jurisdiction of the State [24, 25].

The principle of algorithmic justice. Decisions made with the participation of artificial intelligence must be transparent, verifiable, human-controlled, and comply with the principles of legality, proportionality and protection of human rights [26]. Within electronic jurisdiction, algorithmic justice provides for the

possibility of auditing decision-making models [27], public availability of descriptions of the logic of the functioning of systems, ensuring the possibility of challenging AI-generated results, and mandatory human intervention in cases that have legal consequences [28]. 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 [29, 30].

The principle of decentralized 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 [31, 32]. This principle implies that not only individuals or legal entities, but also platform operators, algorithm owners, smart contract developers, administrators of decentralized systems, and others are responsible for the consequences of digital activities participants of the digital ecosystem [33]. Decentralized responsibility means the collective obligation of actors to ensure transparency, authenticity and security of transactions, to prevent human rights violations, cybercrimes, manipulation or creation of risks to the digital sovereignty of the state [34]. The state, in turn, forms legal mechanisms for controlling such processes through a system of smart regulation, digital audits and international supervision, which guarantees a balance between technological autonomy and legal responsibility [35].

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, ensuring the possibility of cross-border recognition of electronic documents, digital signatures and decisions of judicial or arbitral authorities [36]. Interoperability covers the technical, legal and ethical compatibility of systems, from data exchange protocols to the harmonization of legal procedures and certification standards. formats, standards for electronic identification, cyber protection and preservation of digital evidence, ensuring participation in the global ecosystem of digital justice [37]. 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 [38].

9. Judicial system of electronic jurisdiction

The state ensures the creation and functioning of digital courts, arbitrations and tribunals of a new generation that administer justice in a fully electronic format. These institutions are authorized to consider disputes arising from electronic transactions, blockchain transactions, digital asset transactions, activities in Metaverses, DAOs, smart contracts, and other immersive environments where people, avatars, or autonomous agents interact.

The procedures of such courts take place in virtual courtrooms using videoconferencing technologies, digital identification, cryptographic signature and secure data transmission channels. All case materials — evidence, testimony, protocols, and decisions — are stored in a decentralized state blockchain register of judicial acts, ensuring their immutability, authenticity, and public access.

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.

Digital arbitrations operate based on voluntary submission of the parties, ensuring fast, efficient and cost-effective resolution of disputes in the digital environment, while tribunals function in cases involving global platforms, international digital conflicts and issues of transnational responsibility.

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 rules 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 offenses, violation of the terms of digital licenses or algorithmic agreements.

The 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 creation of digital images of a person without consent.

Within the framework of electronic 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 e-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.

10. Liability in electronic jurisdiction

Violation of the laws of electronic jurisdiction, data manipulation, distortion of digital evidence, unauthorized interference with blockchain records, destruction or forgery of electronic documents, as well as refusal to enforce an electronic court or arbitration award are grounds for legal liability.

Such violations include actions that undermine trust in e-justice systems, impede the implementation 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 offenses 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 e-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 specialized courses, simulations of electronic trials, practice in digital law laboratories, research on algorithmic decisions, and simulation of judicial processes in the Metaverse.

The State also promotes the creation of scientific, analytical and practical platforms that ensure the adaptation of jurisprudence to new forms of e-justice and supports international cooperation in the field of legal regulation of artificial intelligence, Metaverses and the digital economy.

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.

11. Key categories of electronic 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 [39]. It covers both direct participation in transactions and indirect forms of activity — the creation of digital profiles, the functioning of avatars [40], 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 bringing to legal responsibility and is a legally significant element in the process of establishing digital jurisdiction [41]. It considers 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 [42].

Virtual localization 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 considers the geography of servers, the structure of blockchain networks, technical protocols for transmitting information and certification standards, and other factors that determine the conditional "location" of a digital event. Virtual localization allows you to tie actions in a virtual environment to of a specific legal system, even if they are carried out in a decentralized or cross-border format. It provides legal certainty for electronic 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 one within which digital network, protocol or blockchain the transaction, action or transaction is carried out [43]. This concept reflects the logic of distributed systems, in which the legal consequences are determined by the architecture of the algorithm and the rules embedded in it. Algorithmic location implies that it is the code and protocol that perform the function of the normative "legal territory», setting the framework of obligation, responsibility and fulfilment. This approach is especially important in decentralized environments — in particular, in DeFi platforms or metaverse blockchains — where a geographical jurisdiction cannot fully regulate digital legal relations [44]. Algorithmic location provides the prerequisites for the formation of new models of electronic arbitrage, the recognition of smart contract solutions, and the establishment of digital sovereignty of communities [45].

Smart contract binding of rights is an extended legal structure in which the rights and obligations of participants in digital relations are codified in the form of algorithms and implemented automatically without the need for additional intervention of public or private authorities. the application of sanctions in case of violation, the audit of the code for compliance with ethical and legal standards, and the ability to challenge the results in digital arbitration. This approach forms a new level of legal certainty and trust, within which the code acts not only as a technical, but also as a normative instrument of law.

Multi-jurisdictional process is an extended legal category that encompasses 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. prevention of legal conflicts, prioritization of the application of a particular system of law and creation of mechanisms for joint resolution of disputes between subjects of different jurisdictions. It forms the basis for the development of international digital arbitration and new formats of cooperation between states, private platforms and network communities.

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 considers the participation of entities in cross-border blockchain networks [46], Metaverse ecosystems, global data clouds, and decentralized autonomous organizations (DAOs), where legal consequences are formed outside the classical territorial borders of states [47]. Such a status provides for simultaneous subordination to the norms of different jurisdictions, recognition of electronic identifications and transactions in several legal systems, as well as the creation of mechanisms for preventing conflicts and double liability [48]. Cross-border digital legal personality forms the basis for the global interoperability of digital law and contributes to the harmonization of legal regimes in the areas of data, contracts and digital identity [49].

Data jurisdiction is an extended legal regime that determines the application of the law depending on the place of storage, processing, transfer 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 leakage or manipulation of information, as well as ensuring the digital sovereignty of the state [50]. Data jurisdiction considers both technical parameters — geolocation of servers, traffic routing, encryption algorithms — and legal factors: national legislation, international treaties, data localization and 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 the field of GDPR, ISO/IEC and free data flow agreements [51].

A 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 [52, 53]. Such a forum can function in the form of a blockchain platform, a decentralized autonomous organization (DAO) or a smart contract system that automatically enforces arbitral awards based on algorithmic rules [54, 55]. The Virtual Arbitration Forum guarantees neutrality, transparency and efficiency of dispute resolution, 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 [56].

Hybrid jurisdiction is an integrated legal regime that combines elements of physical, digital and algorithmic jurisdiction to resolve complex disputes [57, 58]. It is used in cases where a single legal conflict simultaneously encompasses physical actions, digital transactions and algorithmic processes that interact within a single legal event [59]. An example is a situation where a transaction is concluded in a virtual environment, confirmed by a smart contract in the blockchain, and has consequences in the physical world (supply of goods or provision of services) [60]. A hybrid jurisdiction ensures uniformity of enforcement, prevents collisions, and allows for the use of mixed proof mechanisms: from classic documents to blockchain records and data from the Metaverse. It also provides for the creation of specialized arbitration and court instances capable of integrating different levels of evidence and providing comprehensive technical and legal dispute resolution.

Temporary jurisdictional binding is a special, expansive legal regime that limits the effect of legal norms to a certain period or a specific stage in the execution of a digital transaction or smart contract. It allows you to set time windows of legitimacy for transactions, test legal regimes or experimental digital environments. This approach is used in legal sandboxes, when an innovative technology is allowed to operate only for a certain period, After that, its legal status is subject to review. Time binding ensures the controllability and predictability of digital relationships, reduces the risks of abuse, creates conditions for safe legal experimentation, and makes it possible to respond flexibly to rapid technological changes.

Contextual jurisdiction is an extended legal category that provides for the differentiated application of legal norms depending on the specific environment or technological context in which the digital act originated. Contextual jurisdiction considers the specifics of the digital space — virtual economy, social interaction, algorithmic restrictions — determines the legal status of the participants' actions and the possibility of their appeal in state or supranational institutions. It creates a bridge between the internal rules of digital environments and external legal systems, ensuring a balance between the autonomy of digital platforms and the requirements of public law.

Protocol jurisdiction is a legal regime determined not by territory, but by a standard or technical protocol based on 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 Hyperledger, it is these protocols that set the basic legal framework for the fulfilment of obligations. Protocol jurisdiction considers the peculiarities of network standards — ISO, W3C, TCP/IP, blockchain protocols — their interoperability and security rules, as well as forms the basis for resolving disputes within a specific technological environment. It creates a new level of legal certainty in global decentralized systems, ensuring consistency between technical protocols and legal norms, within which the status of an act is determined not by the territory of the state, but by the protocol that regulates it.

Algorithmic delegation of jurisdiction is a legal model in which part or all the functions of definition, interpretation and application of legal norms are transferred to smart contracts, autonomous algorithms or artificial intelligence agents. monitoring and appealing their decisions, as well as raising issues of ethics, responsibility and legitimacy. Algorithmic delegation can be used in the areas of digital arbitration, resource allocation, automated taxation or control over the execution of contracts, forming hybrid models of human-algorithm interaction in the legal process.

Neurojurisdiction is an expanded legal field that regulates social relations that arise in the process of performing digital actions through neurointerfaces, bionic implants or cyber-physical systems. It covers the issue of legal responsibility for actions initiated by brain signals, determines the legal status of neuroactivity data, as well as mechanisms for protection against manipulation or unauthorized reading of neurodata. Neurojurisdiction is aimed at ensuring a balance between freedom Self-expression of a person in the Brain-Computer Interface environment and the need to ensure the security, privacy and authenticity of transactions. It also considers the ethical aspects of the use of neurotechnologies in medicine, education, labour and management, establishing the normative principles for the harmonious symbiosis of human consciousness with algorithmic systems.

The jurisdiction of digital twins is a complex legal regulation that covers the relationship between an individual and his/her digital reproductions — avatars, simulations, digital clones or digital twins. authenticity, determining the limits of legal autonomy of digital twins, their use for commercial, educational or medical purposes, as well as protection against unauthorized duplication, manipulation or substitution of digital identity. It is aimed at ensuring a balance between a person's freedom to control their digital display and the need to ensure legal certainty in cases where digital twins interact with third parties or acquire signs of independent participants in the digital environment.

Asymmetric jurisdiction is a complex legal phenomenon in which the same digital act, transaction or transaction can acquire different legal status in different legal systems. but at the same time be considered invalid or uncontrolled in the jurisdiction B. Asymmetric jurisdiction creates risks of legal uncertainty, forum shopping and inter-jurisdictional conflicts, but at the same time stimulates the formation of supranational mechanisms for harmonization, unification of legal regimes and the development of international arbitration practices in the field of digital technologies.

Dynamic jurisdiction is a flexible legal regime that automatically changes jurisdiction depending on events in the digital environment, technical updates to smart contracts, or modifications to network protocols. It considers time, context, and technological changes, ensuring that the legal status of transactions, digital acts, and participants is adaptable in real time. Such a mechanism allows you to minimize legal conflicts in fast-paced environments — in the Metaverse or blockchain ecosystems, where the same act can change its jurisdictional affiliation in the process of execution. Dynamic jurisdiction provides for the establishment of clear algorithmic rules for the transition between legal regimes, cryptographic confirmation of each such transition, and mandatory recording of all changes in the distributed ledger.

Electronic personalities and avatars are a legal category that determines the legal status of digital copies of a person (avatars, electronic personalities, digital humanoids) capable of acting independently in the Metaverse [61]. 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 electronic system 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 recognized as valuable and subject to legal regulation. It defines the rules of ownership, use, disposal, establishes mechanisms for confirming ownership and protection against misappropriation through smart contracts and blockchain registries.

Electronic offenses 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 the separation from analog offenses and the establishment of new standards of legal qualification and liability within digital jurisdiction [62].

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 [63].

The e-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 arbitral tribunals. 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 law enforcement environment [64].

Cosmopolitan electronic social relations are a socio-legal category that reflects a new type of social relations in the Metaverse, where there are no traditional state borders, and interaction is based on the principles of voluntariness, mutual consent, and common digital norms. It forms the prerequisites for creating an electronic community with elements of digital citizenship, within which new standards of morality, law, and collective responsibility operate [65].

12. *Legal architecture of electronic jurisdiction*

The legal regulation of social relations in the Metaverse requires a multidimensional electronic jurisdiction, the structure of which covers several interrelated levels — technical, procedural, ethical, and legal. Its architecture is dynamic, network-modular, and capable of self-adaptation, but the foundation of the entire system is the Great Charter of Metaverse Laws (GLM). GLM is the metalegal constitution of the digital world, which acts as the basic legislative framework of the entire Metaverse e-law system [66].

Its purpose is to create a holistic regulatory framework for the digital society, which ensures a balance between innovative development and human rights, integrates ethical standards into the architecture of digital governance and creates conditions for harmonious interaction between people, algorithms and states. The main tasks of the Magna Carta are the development of universal principles of electronic law, coordination of the interstate legal space, ensuring transparency, security, accountability and fairness in all types of digital processes. The purpose of the Charter is to unify the legal foundations of digital existence, increase trust in algorithmic systems, and create a harmonious Metaverse ecosystem in which people, digital avatars, artificial agents, and algorithmic governing bodies interact on the basis of common principles of law, ethics, and responsibility.

Legal architecture of electronic jurisdiction:

The Metaverse Constitution (Magna Carta) 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 [67, 68]. It establishes the principles of ethical governance and legal balance between humans, technology, and the state, and defines mechanisms for data protection, digital dignity, and privacy. In addition, 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 [69].

GLM acts as the architectural core of the Metaverse electronic jurisdiction, forming it as a 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; creating a single semantic database of digital norms (Smart Law Ontology); maintaining the ethicocentric legitimacy of digital processes; creating conditions for global interstate cooperation in the field of e-Justice [70].

The general norms and structure of the laws of the Magna Carta define the principles of digital rulemaking, methods of harmonization between national, corporate and global legal standards, as well as establish the procedure for creating, updating and validating electronic norms [71]. They detail the mechanisms of digital harmonization and modular legislative design, public discussion procedures, ethical evaluation of legal acts and create the basis for automated interpretation of norms in artificial intelligence environment.

Metaverse common law (the **legal, institutional, and technological space of the Metaverse**) forms a system of precedents, norms of behaviour, and algorithmic justice mechanisms [72]. It establishes the principles of equal access to digital justice, defines algorithms for e-dispute resolution, and standards of conduct in virtual environments. Metaverse common law (WM) also regulates the conditions for creating, accumulating, and applying legal precedents in smart contracts, defines mechanisms for harmonization of norms between digital entities and national legal systems, ensuring flexibility, efficiency and fairness in the application of electronic law [73, 74].

The Metaverse judicial system is a multi-layered e-justice architecture that encompasses digital courts, arbitration protocols, ombudsman agents, and Smart Justice modules. storage of evidence, as well as algorithmic models for assessing circumstances and establishing responsibility. Within the framework of Smart Justice, modules for digital mediation, automated arbitration and monitoring of the execution of court decisions are implemented, which ensures the effective, reliable and continuous functioning of e-justice in the Metaverse.

The Metaverse Electronic Office Act (E-Office Act) regulates administrative, procedural, and organizational aspects of managing the activities of electronic entities, defines mechanisms for digital accountability, accounting, and coordination of interaction between institutional agents in the Metaverse [75]. It establishes standards for electronic document management, data management, the procedure for authenticating officials, as well as the rules for the use of digital signatures. In addition, the E-Office Act creates a legal framework for the basis for the implementation of automated administrative processes, electronic licensing systems, auditing, and control over the activities of algorithmic administrations within the Metaverse [76].

The Cross-Border Interaction Regime in the Metaverse establishes the legal framework for the exchange of data, electronic evidence, inter-jurisdictional arbitration, and digital diplomacy [77]. It defines the procedure for the 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. In addition, this regime defines the principles of electronic diplomacy, procedures for settling interstate cyber disputes, as well as mechanisms for cooperation between national judicial systems and Metaverse meta-jurisdictional structures. It also contributes to the formation of a coherent system of legal recognition, in which actions and decisions made in one digital jurisdiction are recognized as valid and have legal force in others.

The Metaverse Code of Fundamental Technical Regulations defines basic standards for security, certification, cryptography, cybersecurity, and interoperability. It sets out requirements for the architecture of digital systems, communication protocols, software verification procedures, and hardware security modules. The Code regulates the application of ISO, IEEE, ITU and other internationally recognized norms, integrating them into a single techno-legal ecosystem of the Metaverse. on the quantum resilience of cryptography, data risk management, the energy efficiency of computing, and the reliability of AI infrastructures.

The Metaverse Identity Management Certificate (Identity Governance Certificate) defines the procedure for creating, verifying and protecting digital identities [78, 79]. It establishes procedures for digital authentication, access rights management, and delegation of identification authority within digital jurisdiction [80, 81]. The certificate also provides mechanisms for protecting personal data, preventing counterfeiting, applying decentralized identifiers (DIDs) and verified credentials (VCs), enabling secure interaction between a person, an organization, and algorithmic actors in the Metaverse environment [82, 83].

The Metaverse Code of Non-Property Electronic Assets regulates the circulation of NFTs, virtual lands, digital works and data as objects of ownership [84]. It defines the legal status of intangible assets, the procedure for their registration, confirmation of authorship and transfer of rights in digital form. The Code establishes the rules for the circulation of tokenized intellectual property, the conditions for the creation and use of digital certificates of ownership, as well as mechanisms for resolving disputes between owners, platforms and developers [85]. Special attention is paid to the inheritance of non-property electronic assets, their storage in decentralized registers, 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 [86].

The Metaverse Criminal Electronic 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 an individual [87]. The Code covers the norms governing the prevention, investigation, and prosecution of cybercrimes, including data integrity violations, manipulation of algorithms, unauthorized access to digital assets, and the use of artificial intelligence for illegal purposes. It establishes levels of responsibility between a person, a developer and an autonomous system, determines the mechanisms of electronic investigation, digital examination and evidentiary verification [88, 89]. In addition, the Code provides for a system of digital rehabilitation, guarantees for the protection of the rights of victims of cybercrimes, and principles of humane treatment in the context of e-justice in the Metaverse [90, 91].

The Metaverse Cyber Security Code provides legal regimes for cyber defence, incident response, and protection of critical digital infrastructure [92, 93]. It defines the principles of cyber resilience, risk management, and continuity of digital operations, establishes standards for responding to cyberattacks, and establishes coordination between public and private entities in the field of cybersecurity [94, 95]. 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 [96]. The issue of liability for violation of cybersecurity norms is separately regulated, mechanisms for certification of specialists and protection algorithms are defined, and forms of cooperation with international structures in the field of global cyber defence are provided [97, 98].

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 conducting information operations and protecting civilians in cyberspace. Particular attention is paid to determining the legal status of cyber warriors, digital volunteers and the introduction of mechanisms for international monitoring and control over compliance with humanitarian law in the context of digital conflicts.

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 systems of electronic justice Metaverse.

Other regulations detail additional areas of regulation of the digital society, including digital citizenship, DAO law, data ecology, ethical certification of algorithms, digital education, artificial diplomacy, regulation of metaverse markets, and digital art. These acts form a single legal framework for adaptation to new socio-technological processes, support interdisciplinary interaction between states, corporations, and digital communities, and create the foundations for the implementation of e-democracy, digital ethics, and sustainable development within the Metaverse.

13. 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 recognized as admissible evidence, provided that three key criteria are met:

1. authenticity — confirmation of the data source using digital signatures, certificates of conformity, hash identifiers and quantum encryption keys;
2. integrity — guaranteeing the immutability of information through blockchain protocols, version control system, and a continuous chain of custody;
3. Legal suitability is the fixation of the date, time, place, digital subject, and algorithm for creating evidence using certified state or international storage platforms.

The category of digital evidence also includes digital testimonies from the Metaverse, audio and video data of XR environments, machine logs of autonomous systems, cryptographic log files, and 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 transactions in the digital environment — including smart contracts, DAO solutions, algorithmic commitments, digital memoranda, and automated transaction scenarios — is recognized as equivalent to offline transactions, provided that a set of requirements specified in the Digital Code is met:

1. party authentication — provided using digital signatures, biometric identifiers, decentralized digital identities (DIDs), or verified smart wallets;
2. voluntariness of will is confirmed by the absence of external algorithmic influence, artificial intelligence manipulation or asymmetric access to information;
3. legal interpretation of the code — the logic of a smart contract should be set out in an understandable legal form, which provides the possibility of litigation or arbitration;
4. transparency of terms — all variable transactions (price, terms, rights, and obligations) must be recorded in an open or verified blockchain ledger;
5. audit and appeal — the parties must have the technical ability to initiate a review or suspension of the execution of a smart contract in case of failures, fraud or a significant change in circumstances.

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 give rise to obligations or changes in legal status. All such actions are governed by the **lex algorithmica principle**, according to which digital codes acquire legal significance subject to their certification and integration into the system of electronic 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:

1. primary (national) liability 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;

2. secondary (cross-border) liability is applied in cases of impact on the rights of foreign citizens, assets or digital platforms, considering the provisions of international treaties, digital conventions and the principles of mutual recognition;

3. 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. Determination of responsibility is carried out through **the mechanism of digital attribution**, which establishes a connection between the action, its technical source and the legal subject. In cases with multi-jurisdictional elements, **a combined model of jurisdictional arbitration can be applied** — with the involvement of the AI regulator, digital courts, and international expert councils. Such a system provides a balance between state sovereignty, global accountability of entities and technological justice in the field of digital legal relations.

Algorithmic jurisdiction. In cases arising from the use 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 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 ones Level:

1. technical level — fixation, auditing, and reproduction of algorithmic actions in the blockchain, verification of digital signatures, hashed, and transaction logs;

2. legal level — legal interpretation of the algorithmic code, its equivalence to traditional norms and determination of the moment of occurrence of legal consequences;

3. The ethical level is the assessment of decisions of autonomous systems for discrimination, opacity, or violation of the principle of human control.

Within the framework of algorithmic jurisdiction, it is envisaged to create **digital arbitration chambers** that consider disputes between smart contract entities, DAOs, or autonomous agents. Each chamber has the right to involve AI experts, conduct coding and verification of evidence, reproduce the logic of the algorithm's functioning, and record the results in a decentralized ledger of decisions.

Priority is given to independent source code audits, transparent action verification mechanisms, and a digital appellate review procedure that strikes a balance between code autonomy and the rule of law.

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 due diligence. 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:

1. risk identification — identification of potential threats to human rights, privacy, data security, algorithmic justice and social impact of the digital system;

2. techno-legal due diligence — analysis of source code, algorithmic logic, data processing protocols and compliance with current legislation;

3. ethical assessment — identifying signs of bias, opacity, discrimination or a decrease in the level of human control (humanintheloop);

4. cyber resilience and security assessment — checking the ability of the system to counteract attacks, prevent leaks and unauthorized access;

5. public reporting is the preparation of an open opinion with recommendations for improving the system and increasing the level of public trust.

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.

14. Institutional architecture

The National Commission for digital jurisdiction is the central coordinating body of digital statehood authorized to ensure the systematic implementation, coordinated interpretation and proper application of the rules 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 e-governance. Her powers include: development and examination of draft regulations in the field of electronic 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 formulates and implements the National digital jurisdiction Strategy, coordinates state participation in international digital initiatives, and provides feedback between the 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 electronic jurisdiction.

Transnational Digital Arbitration is a new generation international institution established 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.

Arbitral awards have the force of digital precedent, are recognized within the framework of signed international conventions and are stored in an open global register of awards, which guarantees their authenticity, immutability and automatic recognition by other jurisdictions. Transnational digital arbitration also performs the functions of digital mediation between states, corporations and autonomous digital entities, acting as a guarantor of the legal balance between national sovereignty, ethical responsibility and the principle of algorithmic justice.

Digital ombudsmen are independent agents operating in the system of digital jurisdiction 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. Their main tasks include: receiving user complaints, initiating investigations, conducting an independent examination of AI systems, participating in digital arbitration as intermediaries and analysts. E-ombudsmen have access to analytical data from public and private platforms, can issue warnings on systemic risks, and generate an annual report on the state of digital rights. In the future, it is planned to create an International Council of Digital Ombudsmen, which will ensure the harmonization of standards and coordination of actions between states, digital arbitrations, and public structures.

The Digital Prosecutor's Office and AI supervisory authorities are specialized institutions responsible for detecting, investigating, and prosecuting digital rights violations, data abuse, cybercrimes, and misconduct by artificial agents. They operate based on open algorithmic law, use their own analytical systems to identify risks in digital transactions, conduct forensic examinations and coordinate activities with national and international law enforcement agencies.

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 includes specialists in the field of law, artificial intelligence, ethics, cybersecurity, sociology and philosophy. The Council conducts legal analysis of new technologies, provides recommendations on legislative regulation, conducts a Social Impact Assessment (FRIA) and forms concepts for legal innovations in the digital sphere.

The International Legal Control Office is an institution that provides audit and supervision of compliance with international standards of digital law. 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 Centre 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 Centre is engaged in the prevention of crisis situations in cyberspace, organizes and conducts negotiations between subjects of digital disputes, and 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 training specialists of a new generation — lawyers, designers, experts in digital jurisdiction (e-jurisdiction) and analysts of artificial intelligence law. The Academy implements programs to prepare judges and investigators to work with digital evidence, organizes and conducts internships in digital courts, and creates international research laboratories on the future of science.

The Digital Justice Controller is an independent analytical and supervisory institute that monitors the state of compliance with digital rights in the world, monitors the activities of corporations and states in the field of algorithmic governance, and analyses trends in technological impact on human rights. The Institute serves as an analytical observatory that prepares annual reports on the state of the balance between technological innovations and fundamental human rights, publishes ratings of transparency of digital states, and provides verified data for international arbitrations, scientific and expert councils and regulatory authorities.

15. Cross-border digital jurisdiction regime

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 harmonization, and automated exchange of decisions between jurisdictions through a decentralized system of interstate registers.

The principle of global compatibility. The cross-border regime of digital jurisdiction is a comprehensive system of harmonization of digital legal norms, procedures and technical standards between states, corporations and international institutions. It is based on the mutual recognition of electronic acts, certificates, smart contracts, court decisions, digital signatures and algorithmic records in blockchains of legal significance.

The aim of the principle is to create a single digital legal space of trust, in which states interact not through traditional paper procedures, but through automated legal interfaces, decentralized registers and standardized exchange protocols. It involves a combination of three interrelated levels of compatibility:

1. **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.).
2. **The legal level** is the harmonization of legislation in the field of digital signatures, electronic documents, blockchain records, smart contracts, identity management, XR technologies, digital identity, etc.
3. **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 decentralized 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 adopted within the framework of digital jurisdiction is carried out through a multi-level system of digital certification:

1. Verification of the authenticity of the digital signature and smart contract code of the solution.
2. Identification of the digital entity against whom the decision has been rendered.
3. Automatic entry of the decision into the international register with fixation of date, hashidentifier 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 settlement, exchange of evidence, joint investigations of cyber incidents, and mutual enforcement of judicial acts. Such agreements are stored in the international blockchain

registry 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 organizations. 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.

Each such agreement is concluded in the form of a smart contract, which contains certain terms of cooperation: an algorithm for mutual access to data, response time limits, privacy protection mechanisms, encryption standards, and evidence storage procedures. If the established conditions are met, the transaction is activated automatically, initiating the actions of the relevant national authorities and recording all transactions in the international blockchain registry.

These agreements have the status of cross-border smart contracts, which are recognized as a source of international digital law. They not only ensure the legal validity of the decisions made but also form a transparent system of cooperation between states. To increase the effectiveness of international digital cooperation, it is envisaged to create a Register of Digital Conventions, which records all existing agreements, their participants, subject of legal regulation, established ethical standards and the results of the audit of their implementation.

In addition, digital agreements may contain automated sanctions protocols that are activated in case of violation of contractual terms or non-fulfilment of obligations by the parties. Such protocols are implemented through smart contracts and enforce techno-legal restrictions, such as temporarily freezing digital assets, blocking access to global ledgers, or restricting transactions within the relevant digital jurisdiction.

Thus, digital agreements are gradually turning into the core of the regulatory and legal infrastructure of cross-border jurisdictions, ensuring a balance between state sovereignty, data protection and the efficiency of international legal response.

Electronic 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 determine a special procedure for considering cases with an international element. To ensure technological compatibility and legal certainty, special procedural standards apply in such cases:

1. 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;
2. The use of quantum keys to encrypt evidence and secure transfer of procedural documents between jurisdictions;
3. Conducting court hearings in XR format environments with full fixation of digital data, biometric identifiers and evidentiary materials;
4. Automated enforcement of judgments through a decentralized 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 considers 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. For this purpose, joint ethics councils, technical committees on cyber resilience and mechanisms for rapid response to cross-border incidents are being established.

Thus, the cross-border digital jurisdiction regime acts as a multi-level architecture of digital legal unity, combining national, regional and global levels of governance, integrating state and corporate systems, international judicial and arbitration institutions, as well as electronic identification networks. It forms not only a common infrastructure for data exchange and mutual recognition of decisions, but also a normative ethical framework for compliance with digital human rights.

This regime provides for the creation of a single legal platform for digital interoperability, which ensures secure interaction between jurisdictions in real time, automated updating of regulations and coordination between national regulators. It includes digital attribution mechanisms, global certification centres, registers of cross-border agreements, and joint cyber defence protocols.

As a result, a new generation of international electronic legal order is being formed — flexible, transparent, ethically verified and technologically protected. It strikes a balance between the digital sovereignty of states, the freedom of global interaction, and the rule of algorithmic law, turning digital jurisdiction into the foundation of trust in the global digital civilization.

Conclusions.

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. Thus, digital jurisdiction appears as a new type of public law infrastructure, in which the boundaries of the legal field are determined not by geography, but by digital protocols of trust and authentication.

The digital jurisdiction model is a structural legal system. The article substantiates the feasibility of presenting digital jurisdiction as a model consisting of four interrelated levels: technical — covering data infrastructure, blockchain systems, artificial intelligence and digital security mechanisms; procedural — which includes algorithmic justice, digital arbitration, and Smart Justice modules; ethical — based on the principles of human dignity, digital autonomy and non-discrimination; and legal — aimed at the formation of digital governance codes, standards and regulations. This model provides an opportunity to implement the concept of digital law-making using 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.

Summarizing the results of the study, it can be argued that digital jurisdiction is moving from the plane of theoretical searches to the sphere of applied law-making and appears as an operational model of the digital law order of the future — a combination of algorithmic governance, network ethics and legal legitimacy in a single metasystem capable of evolving synchronously with technological development. The proposed model not only reflects the current state of scientific discussion but also outlines a new vector for the development of legal science — from textual law to metalegal code, from territorial statehood to functional digital sovereignty.

In this sense, digital jurisdiction appears not only as an object of scientific research, but as a tool for civilizational 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.

REFERENCES

[1] Kostenko O. V. Electronic Jurisdiction, Metaverse, Artificial Intelligence, Digital Personality, Digital Avatar, Neural Networks: Theory, Practice, Perspective. World Science. 2022. 1(73). P. 1-13.

2Barlow, J. P. (1996). Declaration of the Independence of Cyberspace. Available at: https://www.eff.org/cyberspace-independence.

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

4 Lessig, L. (1998). The Laws of Cyberspace. Taiwan Net ’98 Conference. Available at: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf.

[5] Kaddoura, S., & Husseiny, F. (2023). The rising trend of Metaverse in education: challenges, opportunities, and ethical considerations. *PeerJ Computer Science*, 9. https://doi.org/10.7717/peerj-cs.1252.

[6] Dwivedi, Y., Hughes, L., Baabdullah, A., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., Janssen, M., Kim, Y., Kim, J., Koos, S., Kreps, D., Kshetri, N., Kumar, V., Ooi, K., Papagiannidis, S., Pappas, I., Polyviou, A., Park, S., Pandey, N., Queiroz, M., Raman, R., Rauschnabel, P., Shirish, A., Sigala, M., Spanaki, K., Tan, G., Tiwari, M., Viglia, G., & Wamba, S. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.*, 66, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542.

[7] Mascitti, M. (2024). The Metaverse impact on the politics means. *Comput. Law Secur. Rev.*, 55, 106037. https://doi.org/10.1016/j.clsr.2024.106037.

[8] Johnson, David Reynold and Post, David G., Law and Borders - the Rise of Law in Cyberspace. Stanford Law Review, Vol. 48, p. 1367, 1996, Available at SSRN: https://ssrn.com/abstract=535 or http://dx.doi.org/10.2139/ssrn.535
[9] 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. *Comput. Law Secur. Rev.*, 53, 105965. https://doi.org/10.1016/j.clsr.2024.105965.
[10] Yang, Y. (2024). Analysis on the Extraterritorial Expansion and Conflict of Digital Prescriptive Jurisdiction. *Dispute Settlement*. https://doi.org/10.12677/ds.2024.101017.
[11] Hildebrandt, M. (2013). Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace. *University of Toronto Law Journal*, 63, 196-224. https://doi.org/10.3138/UTLJ.1119.
[12] Li, K. (2022). Reconceiving Extraterritorial Jurisdiction. *German Yearbook of International Law*. https://doi.org/10.5771/9783748933212.
[13] Saidov, B. (2025). LEGAL REGULATION OF METAVERSES: ISSUES OF JURISDICTION AND INTELLECTUAL PROPERTY PROTECTION IN VIRTUAL WORLDS. *Jurisprudence*. https://doi.org/10.51788/tsul.jurisprudence.5.2./hlrq3208.
[14] Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24, 537-550. https://doi.org/10.1017/glj.2023.24.
[15] Leontiev, L. (2024). Conceptualising Extraterritoriality. Public International Law and Private International Law Considerations. *Global Jurist*, 24, 119-155. https://doi.org/10.1515/gj-2023-0128.
[16] Sullivan, C., & Tyson, S. (2023). A global digital identity for all: the next evolution. *Policy Design and Practice*, 6, 433-445. https://doi.org/10.1080/25741292.2023.2267867.
[17] Sullivan, C. (2018). Digital identity - From emergent legal concept to new reality. *Comput. Law Secur. Rev.*, 34, 723-731. https://doi.org/10.1016/J.CLSR.2018.05.015.
[18] 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.
[19] Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, 63, 603-613. https://doi.org/10.1007/s12599-021-00722-y.
[20] 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.
[21] 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 PE/68/2023/REV/1 https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng?utm_source=chatgpt.com
[22] Michałkiewicz-Kądziela, E., & Milczarek, E. (2022). Legal boundaries of digital identity creation. *Internet Policy Review*. https://doi.org/10.14763/2022.1.1614.
[23] Sullivan, C. (2013). Is Your Digital Identity Property? An Examination of Digital Identity in the Era of e-Government and Digital Citizenship.
[24] 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.
[25] Tammpuu, P., & Masso, A. (2019). Transnational Digital Identity as an Instrument for Global Digital Citizenship: The Case of Estonia's E-Residency. *Information Systems Frontiers*, 21, 621-634. https://doi.org/10.1007/s10796-019-09908-y.
[26] Sachan, S., & Liu, X. (2024). Blockchain-based auditing of legal decisions supported by explainable AI and generative AI tools. *Eng. Appl. Artif. Intell.*, 129, 107666. https://doi.org/10.1016/j.engappai.2023.107666.
[27] Chiao, V. (2019). Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice. *International Journal of Law in Context*, 15, 126-139. https://doi.org/10.1017/S1744552319000077.
[28] 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.
[29] 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.
[30] Koulu, R. (2020). Proceduralizing control and discretion: Human oversight in artificial intelligence policy. *Maastricht Journal of European and Comparative Law*, 27, 720-735. https://doi.org/10.1177/1023263X20978649.
[31] Napieralska, A., & Kepczynski, P. (2024). Redefining Accountability: Navigating Legal Challenges of Participant Liability in Decentralized Autonomous Organizations. *ArXiv*, abs/2408.04717. https://doi.org/10.48550/arXiv.2408.04717.
[32] Dwivedi, V., Norta, A., Wulf, A., Leiding, B., Saxena, S., & Udokwu, C. (2021). A Formal Specification Smart-Contract Language for Legally Binding Decentralized Autonomous Organizations. *IEEE Access*, 9, 76069-76082. https://doi.org/10.1109/ACCESS.2021.3081926.
[33] 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.
[34] Truong, N., Lee, G., Sun, K., Guitton, F., & Guo, Y. (2021). A Blockchain-based Trust System for Decentralised Applications: When trustless needs trust. *ArXiv*, abs/2101.10920. https://doi.org/10.1016/J.FUTURE.2021.05.025.

[35] Panagou, E., & Vavalis, M. (2020). Towards an open and decentralized case law curation ecosystem. *PLoS ONE*, 15. https://doi.org/10.1371/journal.pone.0240041.
[36] 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.
[37] Jimenez-Gomez, C. (2012). Implementing Interoperability in E-Justice's Criminal Area.
[38] Malik, 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.2023.3293529.
[39] 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.
[40] Raposo, V. (2024). Beyond pixels and profiles: unveiling the legal identity of avatars in the metaverse. *Interactive Entertainment Law Review*. https://doi.org/10.4337/ielr.2024.02.04.
[41] Noval, S., & Maaruf, I. (2024). Toward a Comprehensive Cyber Law Framework: Assessing Avatar Legal Liability. *China and WTO Review*. https://doi.org/10.52152/cwr.2024.10.1.07.
[42] Barfield, W., & Williams, A. (2018). The law of virtual reality and increasingly smart virtual avatars. 2-43. https://doi.org/10.4337/9781786438591.00008.
[43] Watters, C. (2023). When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment. *Laws*. https://doi.org/10.3390/laws12020033.
[44] 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*. https://doi.org/10.19184/jkph.v4i2.53366.
[45] De Filippi, P., & Hassan, S. (2016). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. *First Monday*, 21. https://doi.org/10.5210/FM.V21I12.7113.
[46] Garcia-Teruel, R., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Comput. Law Secur. Rev.*, 41, 105543. https://doi.org/10.1016/J.CLSR.2021.105543.
[47] Tumakov, A. (2024). Digital and Virtual Objects of Modern Civil Turnover: The Issue of Differentiation of Concepts. *Lex Russica*. https://doi.org/10.17803/1729-5920.2024.212.7.030-038.
[48] 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, 919-958. https://doi.org/10.1080/14650045.2022.2050070.
[49] Quinn, J. (2021). Geo-location technology: restricting access to online content without illegitimate extraterritorial effects. *International Data Privacy Law*. https://doi.org/10.1093/idpl/ipab016.
[50] Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24, 537-550. https://doi.org/10.1017/glj.2023.24.
[51] Quinn, J. (2021). Geo-location technology: restricting access to online content without illegitimate extraterritorial effects. *International Data Privacy Law*. https://doi.org/10.1093/idpl/ipab016.
[52] (2021). OUP accepted manuscript. *Journal of International Dispute Settlement*. https://doi.org/10.1093/jnlids/idab025.
[53] Okezie, P. (2024). Resolving Smart Contract Disputes Through Blockchain Arbitration. *Arbitration: The International Journal of Arbitration, Mediation and Dispute Management*. https://doi.org/10.54648/amdm2024013.
[54] Wiegandt, D. (2022). Blockchain and Smart Contracts and the Role of Arbitration. *Journal of International Arbitration*. https://doi.org/10.54648/joia2022029.
[55] Gabuthy, Y. (2023). Blockchain-Based Dispute Resolution: Insights and Challenges. *Games*, 14, 34. https://doi.org/10.3390/g14030034.
[56] Aouidef, Y., Ast, F., & Deffains, B. (2021). Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects. 4, 1-8. https://doi.org/10.3389/fbloc.2021.564551.
[57] Allouzi, 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*. https://doi.org/10.5267/j.ijdns.2023.8.001.
[58] Gronic, I. (2023). Transforming Digital Dispute Resolution in India. *RUDN Journal of Law*. https://doi.org/10.22363/2313-2337-2023-27-4-1113-1124.
[59] Atiyah, G., Ibrahim, A., & Jasim, A. (2024). Enforcement of smart contracts in cross-jurisdictional transactions. *International Journal of Law and Management*. https://doi.org/10.1108/ijlma-06-2024-0220.
[60] Szabo, J., Bernard, C., & Philip, L. (2024). Legal Implications and Challenges of Blockchain Technology and Smart Contracts. *Computer Life*. https://doi.org/10.54097/ztn2w848.
[61] Global, R., Oleksii, A., Oleksii, D., & Dmytro, Z. (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*. https://doi.org/10.31435/rsglobal_ijitss/30062024/8141.

[62] Qin, H., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *ArXiv*, abs/2210.06134. https://doi.org/10.1057/s41599-024-04266-w.
[63] Svantesson, D. (2013). A 'layered approach' to the extraterritorality of data privacy laws. *International Data Privacy Law*, 3, 278-286. https://doi.org/10.1093/IDPL/IPT027.
[64] 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*. https://doi.org/10.46282/blr.2022.6.2.316.
[65] Riva, G., Wiederhold, B., & Mantovani, F. (2023). Searching for the Metaverse: Neuroscience of Physical and Digital Communities. *Cyberpsychology, Behavior and Social Networking*, 27, 9-18. https://doi.org/10.1089/cyber.2023.0040.
[66] 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*. https://doi.org/10.46282/blr.2022.6.2.316.
[67] Dwivedi, Y., Hughes, L., Baabdullah, A., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., Janssen, M., Kim, Y., Kim, J., Koos, S., Kreps, D., Kshetri, N., Kumar, V., Ooi, K., Papagiannidis, S., Pappas, I., Polyviou, A., Park, S., Pandey, N., Queiroz, M., Raman, R., Rauschnabel, P., Shirish, A., Sigala, M., Spanaki, K., Tan, G., Tiwari, M., Viglia, G., & Wamba, S. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *Int. J. Inf. Manag.*, 66, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542.
[68] Nurudeen, M., Latilo, A., Imosemi, H., & Imosemi, Q. (2024). Integrative legal operating model design: Incorporating ai and blockchain in legal practice. *Global Journal of Research in Multidisciplinary Studies*. https://doi.org/10.58175/gjrms.2024.2.1.0036.
[69] Bibri, S., & Allam, Z. (2022). The Metaverse as a virtual form of data-driven smart cities: the ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society. *Computational Urban Science*, 2. https://doi.org/10.1007/s43762-022-00050-1.
[70] 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.
[71] Uddin, M., Manickam, S., Ullah, H., Obaidat, M., & 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.
[72] Allouzi, 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*. https://doi.org/10.5267/j.ijdns.2023.8.001.
[73] Watts, J. (2025). Law in the Metaverse. . https://doi.org/10.5040/9781526530783.
[74] 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.
[75] Chen, Z. (2023). Metaverse office: exploring future teleworking model. *Kybernetes*, 53, 2029-2045. https://doi.org/10.1108/k-10-2022-1432.
[76] 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.
[77] 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.
[78] Kostenko, O. (2021). IDENTIFICATION DATA MANAGEMENT: LEGAL REGULATION AND CLASSIFICATION. *Scientific Journal of Polonia University.* 43(6), 198-203. DOI: https://doi.org/10.23856/4325
[79] 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.
[80] Kostenko, O. (2021). V. Identification of IoT: Origins of the Problem of Legal Regulation of Identity Data Management. *Juris Europensis Scientia,* 1, 77-83. DOI: https://doi.org/10.32837/chern.v0i1.177.org/10.32837/chern.v0i1.177
[81] Kostenko, O. (2021). Management of Identification Data: Legal Regulation and Classification. *Young scientist*. 3(91), 90-94. DOI: https://doi.org/10.32839/2304-5809/2021-3-91-21
[82] 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.
[83] Kostenko, O. (2021). Paradigms of identity data management in the light of the development of IoT devices and artificial intelligence. *Amparo*. 3, 42-47. DOI: https://doi.org/10.26661/2616-9444-2021-3-06
[84] Wyczik, J. (2024). The rise of the metaverse: tethering effect and intellectual property of crypto tokens. *Journal Of Intellectual Property Law and Practice*. https://doi.org/10.1093/jiplp/jpad124.
[85] 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, 1-20. https://doi.org/10.1145/3585387.

[86] 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/m3056.
[87] Qin, H., Wang, Y., & Hui, P. (2022). Identity, Crimes, and Law Enforcement in the Metaverse. *ArXiv*, abs/2210.06134. https://doi.org/10.1057/s41599-024-04266-w.
[88] Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters, 1-58. https://doi.org/10.1007/978-3-030-50613-1_1.
[89] 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. https://doi.org/10.48550/arXiv.2205.12911.
[90] Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). METAVERSE: MODEL CRIMINAL CODE. *Baltic Journal of Economic Studies*. https://doi.org/10.30525/2256-0742/2023-9-4-134-147.
[91] Arnell, P., & Faturoti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 37, 29-51. https://doi.org/10.1080/13600869.2022.2061888.
[92] Pooyandeh, M., Han, K., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences*. https://doi.org/10.3390/app122412993.
[93] Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Comput. Ind. Eng.*, 149, 106829. https://doi.org/10.1016/j.cie.2020.106829.
[94] 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, 176. https://doi.org/10.3390/fi16050176.
[95] Sable, N. (2024). Cybersecurity Policies for Critical Infrastructure: Legal Mandates and Network Protection Requirements. *Netw. Secur.*, 2024, 25-31. https://doi.org/10.70985/ns.v2024i8.51.
[96] Srinivas, J., Das, A., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.*, 92, 178-188. https://doi.org/10.1016/j.future.2018.09.063.
[97] Sebastian, G. (2023). A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. *Int. J. Secur. Priv. Pervasive Comput.*, 15, 1-14. https://doi.org/10.4018/ijsppc.315591.
[98] Radanliev, P. (2024). Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. *Frontiers Blockchain*, 7. https://doi.org/10.3389/fbloc.2024.1359130.