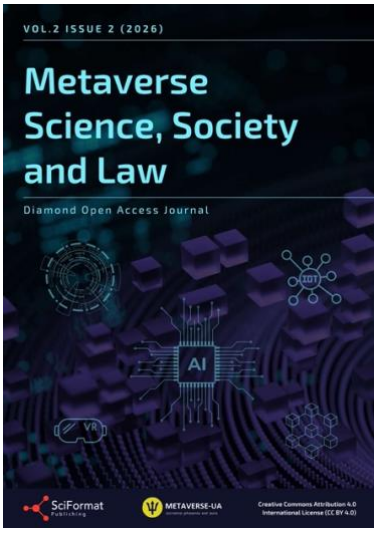


Metaverse Science, Society and Law

Vol. 2, Issue 2 (2026)

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	TECHNICAL AND LEGAL DEFINITIONS AS A BASIS OF MODERN DIGITAL LAW AND DIGITAL JURISDICTION: A MODEL ALGORITHM OF AI DESIGN TECHNICAL AND LEGAL NORMS
DOI	https://doi.org/10.69635/mssl.2026.2.2.41
RECEIVED	15 January 2026
ACCEPTED	30 April 2026
PUBLISHED	18 May 2026
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

© The author(s) 2026.
This article is published as open access under the Creative Commons Attribution 4.0 International License (CC BY 4.0), allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

TECHNICAL AND LEGAL DEFINITIONS AS A BASIS OF MODERN DIGITAL LAW AND DIGITAL JURISDICTION: A MODEL ALGORITHM OF AI DESIGN TECHNICAL AND LEGAL NORMS

Oleksii Kostenko
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

Nataliya Onishchenko
D.Sc. (Law), Professor, Academician of the National Academy of Legal Sciences of Ukraine, Deputy Director of the Institute of State and Law named after V.M. Koretsky National Academy of Sciences of Ukraine, Honored Lawyer of Ukraine, Ukraine
ORCID ID: 0000-0002-1671-2139

Dmytro Zhuravlov
D.Sc. (Law), Professor, Office of the President of Ukraine, Honored Lawyer of Ukraine, Ukraine
ORCID ID: 0000-0002-2205-6828

ABSTRACT

The rapid convergence of artificial intelligence, data management, digital identity, blockchain infrastructures, smart contracts, digital twins, immersive environments, and Metaverse/Web 4.0 platforms has revealed the structural insufficiency of the classical legal conceptual apparatus. The traditional legal definition mostly stabilizes the meaning of the term within the normative text, while digital law requires definitions that can simultaneously reflect technological functionality, algorithmic implications, interoperability requirements, evidence, responsibility and jurisdictional linkage. The article aims to substantiate technical and legal definitions as initial modules for the design of technical and legal norms (TLN) — a new type of normative construction of modern information law. The research methodology combines doctrinal analysis, comparative legal method, legal and linguistic analysis, legal semiotics, system-structural method, normative modeling and AI-assisted legal modeling under mandatory human control. The article shows that modern digital regulatory acts, including the EU AI Act, GDPR, Digital Services Act, Data Act, eIDAS 2.0, Cyber Resilience Act, and MiCA, are already built around complex technical and legal definitions that define the boundaries of rights, obligations, risks, compliance, responsibility, and jurisdiction. The scientific novelty lies in the proposed ten-stage algorithm for designing a TLN with the use of AI and the mandatory participation of a human expert.
Highlights:
1) Technical and legal definitions are infrastructural elements of digital law;
2) Technical and legal norms transform technological phenomena into rights, obligations, guarantees and mechanisms of responsibility;
3) AI can support legal modeling, but does not replace a human expert;
4) Modern EU digital legislation demonstrates the growing importance of technical and legal definitions;
5) A ten-stage algorithm for designing the TLN as a new type of normative construction of information law is proposed.

KEYWORDS

AI, Information Law, Digital Transformation, Technical and Legal Definitions, Technical and Legal Norms, Digital Law, Digital Jurisdiction, Artificial Intelligence, Digital Code

CITATION

Oleksii Kostenko, Nataliya Onishchenko, Dmytro Zhuravlov. (2026) Technical and Legal Definitions as a Basis of Modern Digital Law and Digital Jurisdiction: A Model Algorithm of AI Design Technical and Legal Norms. *Metaverse Science, Society and Law*. Vol. 2, Issue 2. doi: 10.69635/mssl.2026.2.2.41

COPYRIGHT

© The author(s) 2026. This article is published as open access under the **Creative Commons Attribution 4.0 International License (CC BY 4.0)**, allowing the author to retain copyright. The CC BY 4.0 License permits the content to be copied, adapted, displayed, distributed, republished, or reused for any purpose, including adaptation and commercial use, as long as proper attribution is provided.

1. Introduction

The digital transformation of society has not only created new objects of legal regulation. It has changed the internal grammar of legal regulation, since law increasingly deals not with classical material things, institutional powers or traditional legal facts, but with hybrid technological and legal phenomena. Such phenomena include artificial intelligence systems, algorithmic decisions, digital identity wallets, recommendation systems, digital twins, smart contracts, crypto assets, biometric systems, avatars, synthetic content, autonomous agents, and immersive environments.

This transformation creates a fundamental problem for legislative technique. The ordinary legal definition has historically been oriented towards clarifying the meaning of the term within the law. In the field of digital law, the definition should perform a much more complex function: to establish whether a technological object falls under the legal regime; identify the responsible entity; determine the legal consequences of the functioning of the technology; provide compliance checks; maintain cross-border interoperability; and, in rare cases, be suitable for machine reading or algorithmic operationalization.

That is why our study proceeds from the thesis that digital law requires a transition from technical and legal definitions to technical and legal norms. The technical-legal definition identifies a technological phenomenon in legally relevant features. The technical-legal norm, or TLN, goes further: it transforms this phenomenon into a normative structure that contains rights, obligations, prohibitions, permits, procedural guarantees, documentation requirements, audits, evidentiary standards, criteria of responsibility and jurisdictional connections.

Accordingly, the article does not consider definitions as a secondary element of legal terminology. On the contrary, she proposes to interpret them as the initial module of the new normative engineering of information law. In the digital age, the legislator can no longer be satisfied with linguistic precision. It should design norms that can work in technological, algorithmic, platform, and cross-border environments.

The central thesis of the study should be formulated as follows: in modern information law, technical and legal definitions constitute the conceptual basis of technical and legal norms, and the TLN is a new type of normative construction, with the help of which technological reality is transformed into a legally significant, demonstrably suitable and jurisdictionally relevant legal form.

The relevance of this approach is confirmed by modern digital legislation. The EU AI Act, GDPR, Digital Services Act, Data Act, eIDAS 2.0, Cyber Resilience Act, and MiCA demonstrate that much of digital regulation is already built around complex definitive constructs. They define not only the meaning of terms, but also the boundaries of the market, responsibility, compliance, risks and supervisory powers.

At the same time, modern legislative practice remains fragmented. Definitions are created by sectors: separately for AI, separately for personal data, separately for platforms, separately for cybersecurity, separately for crypto assets. However, digital law as a complex normative space requires a common methodology for the construction of TLN, capable of combining technical precision, legal certainty and human control.

This approach is especially important for the doctrine of digital jurisdiction. Digital jurisdiction cannot be reduced to the territorial reference of the server, the place of registration of the platform or the citizenship of the user. It requires legal recognition of digital entities, digital objects, digital actions, algorithmic decisions, platform events, and digital evidence. Such recognition is impossible without technical and legal definitions and TLN.

The purpose of our study is to substantiate technical and legal norms as a new type of normative construction of modern information law and to develop an AI-assisted and human-controlled algorithm for their design.

The objectives of the study are: to reveal the nature of the technical and legal definition; to distinguish it from the usual legal definition; to show the current state of use of such definitions in legislation; to justify the transition from definition to norm; to propose an algorithm for creating a TLN; to determine the role of AI and a human expert; to show the importance of the TLN for digital jurisdiction and the digital code.

The structure of the work follows this logic. First, the theoretical foundations of definitions and norms are considered. Next, modern legislation is analyzed. Then, the distinction between the technical definition, the technical-legal definition and the technical-legal norm is formulated. The central block is a ten-stage algorithm for designing a TLN using AI under mandatory human control. The final chapters are devoted to digital jurisdiction, the digital code, discussion, conclusions, tables and captions to figures.

2. Theoretical foundations: from legal definitions to technical and legal norms

The problem of legal definitions has traditionally been studied within the framework of legislative technique, the theory of interpretation of law, legal language, legal logic and the general theory of law. The classical approach proceeds from the fact that the definition should ensure the unambiguity of the term, reduce the risk of contradictory interpretation, determine the scope of application of the legal regime and ensure the internal consistency of the normative act.

Many studies record the uncertainty and instability of the categorical apparatus in digital relations, through slang, borrowing, and technical terms without clear legal [1]qualifications.

For traditional legislation, this function was sufficient. For example, the definition of a contract, property, official or administrative service mainly provides a legal distinction between related legal categories. In digital law, the situation is different. Here, the term often does not come from legal doctrine, but from technical, engineering, information or platform practice. Therefore, the legislator must not only explain the term, but also legally transform the technological phenomenon.

This transformation means that a technical concept cannot be automatically transferred to law[2]. For example, the concepts of "artificial intelligence model", "API", "token", "biometric template", "digital twin" or "avatar" in the technical documentation do not have the same boundaries and consequences as in law. The technical description answers the question of how the system works. A legal norm answers the question of what rights, obligations, risks, responsibilities and procedural guarantees arise in connection with its functioning.

Therefore, the technical-legal definition has a hybrid nature. It is at the same time an element of legal language, an instrument of normative qualification, a mechanism of technological relevance and a prerequisite for law enforcement. Its task is to make a technological object visible to law without losing its essential technical properties[3].

The technical-legal norm is the next level of this evolution. If the definition answers the question of what exactly the subject of regulation is, then the TLN answers the question of how this phenomenon is regulated. That is why the TLN should contain not only a conceptual block, but also a normative disposition, subject composition, procedures, guarantees, mechanisms of proof and responsibility.

In this respect, the proposed concept differs from the usual approach to legal definitions. It is not only about improving the legal language, but about creating a new type of normative construction that is able to function in the conditions of algorithmic dynamics, technological variability and cross-border digital interaction. The differences between ordinary legal definitions and technical-legal definitions are systematized in Table. 1.

Table 1. Difference between ordinary legal definitions and technical legal definitions

Criterion	Ordinary legal definition	Technical and legal definition	Significance for digital law
Purpose	Clarifies the meaning of the term within the framework of the law	Transforms a technological phenomenon into a legally significant category	Defines the boundaries of the digital legal regime
Source of content	Legal doctrine, law, judicial practice	Law, technology, standards, system architecture, risk	Ensures technological correctness
Function	Mostly explanatory	Explanatory, technical, evidentiary, procedural, jurisdictional	Allows you to adjust real digital systems
Legal consequence	Helps interpret the norm	Triggers rights, obligations, compliance, responsibility	Becoming a regulatory trigger
Machine readability	Usually not considered	Can be laid down as an additional requirement	Supports automated governance
Interoperability	Limited by the boundaries of law and order	Matters for platforms, states, and cross-border systems	Required for digital jurisdiction

The key methodological problem is the correlation between the stability of law and the variability of technology[4]. The law should be stable enough to provide legal certainty, but at the same time flexible enough not to become obsolete after each software update or change in the technical standard[5]. That is why TLN

should not copy the technical standard. It should record legally significant features of a technological phenomenon that remain relevant even when a specific technical implementation changes.

For example, in the field of AI, the law should regulate not specific model architecture, but legally significant characteristics: autonomy, ability to form conclusions, impact on a person, risk to rights and freedoms, the possibility of human oversight, documentation, audit, explainability, and subject of responsibility. In the field of digital identity, not only the cryptographic parameters of the system have legal significance, but also authentication, personality attributes, evidence of the action, the legal force of electronic representation and the appeal mechanism.

That is why the technical and legal norm should be designed as a multi-level structure (Fig. 1)

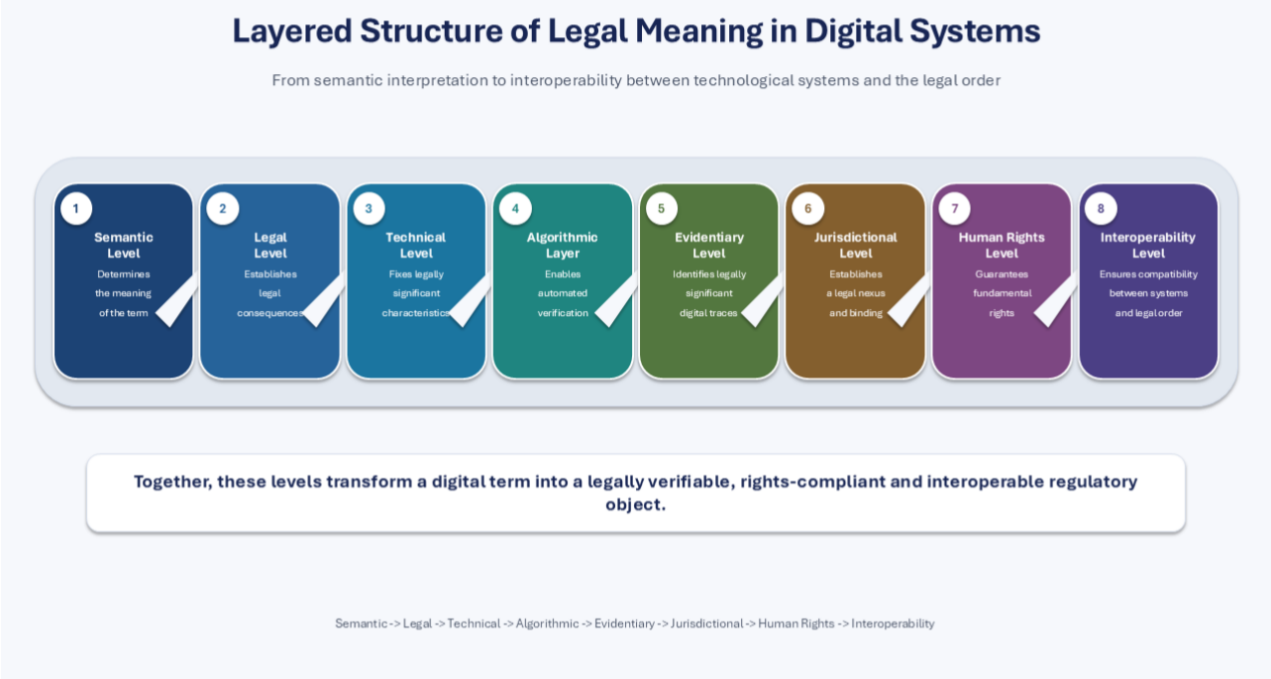


Fig. 1. *Technical and legal norm as a multi-level structure.*

Its semantic level determines the meaning of the term; the legal level establishes the consequences; the technical level fixes legally significant characteristics; the algorithmic layer provides the possibility of automated verification; the evidentiary level determines which digital traces have legal significance; the jurisdictional level establishes a legal binding; the human rights level guarantees fundamental rights; The interoperable level ensures compatibility between systems and law and order.

Thus, the concept of the TLN allows you to rethink the conceptual apparatus of digital law. The definition ceases to be just an introductory provision of the law and becomes part of the regulatory infrastructure. This is the first level of scientific novelty of the article.

3. Current state of legislation: technical and legal definitions in digital acts

An analysis of modern digital legislation shows that technical and legal definitions have become the main way of constructing regulatory regimes. The legislator can no longer regulate digital phenomena through abstract general categories.[6]

The EU AI Act is one of the most illustrative examples of this approach. Its regulatory architecture depends on the definitions of "AI system", "provider", "deployer", "high-risk AI system", "general-purpose AI model", "biometric identification system", "emotion recognition system" and other categories. These definitions are not neutral. They determine whether the subject is subject to the requirements of risk management, technical documentation, transparency, human supervision, registration, post-marketing monitoring and liability.

The peculiarity of the AI Act is that the definition acts as a regulatory gateway. If the system falls under the concept of AI system, it is included in a certain legal regime.[7]

The GDPR demonstrates another, but no less important variant of technical and legal definitive architecture. The concepts of "personal data", "processing", "controller", "processor", "profiling", "pseudonymisation", "biometric data" and "genetic data" define not only terms, but also the boundaries of fundamental rights, obligations of controllers, legal bases for processing, risk assessment, rights of data subjects and competence of supervisory authorities[8].

The GDPR shows that the technical and legal definition can be law-triggering. When information is recognized as personal data, the entire data protection regime arises[9]. When an entity qualifies as a controller, it is assigned a set of responsibilities. This means that the definition works as a normative trigger.

The Digital Services Act uses technical and legal definitions to build regulation of the platform economy[10]. It distinguishes between intermediary services, hosting services, online platforms, online search engines, very large online platforms and very large online search engines[11],[12].The definition of recommender system is of particular importance, since recommendation algorithms affect the visibility of information, user behavior, political communication, commercial promotion and platform power.

In the DSA, the technical ranking or recommendation mechanism turns into a legally significant object of regulation[13]. This means that the legislator recognizes that the algorithmic architecture of the platform can create legal risks and requires separate responsibilities of transparency, accountability, and control.

The Data Act demonstrates the importance of definitions for the data economy. The concepts of "connected product", "related service", "data holder", "user", "product data" and "readily available data" define who has access to data, who controls its use, what responsibilities manufacturers and suppliers have, and how fair access to data is ensured[14]. Here, the definition distributes not only legal roles, but also economic power over digital resources[15].

eIDAS 2.0 and the European Digital Identity Wallet regulation are of particular importance for digital jurisdictions [16]. Electronic identification [17], trust services [18], qualified electronic signatures [19], attribute attestations and digital identity wallets form the infrastructure of legal facial recognition in the digital environment. Without such definitions, it is impossible to establish who exactly acts in the digital space, whether the action has legal force, whether it can be evidence, and which legal order recognizes its consequences[20].

The Cyber Resilience Act translates cybersecurity from the plane of technical recommendation to the plane of legal [21]obligation. [22]The concepts of "product with digital elements", "vulnerability", "software", "hardware", "manufacturer" and "placing on the market" determine which objects are subject to cybersecurity requirements, who is responsible for vulnerabilities, what conformity assessment procedures are applied and what consequences occur for violations[23],[24].

The MiCA Regulation shows how technical and legal definitions stabilize volatile digital financial markets[25]. The concepts of "crypto-asset", "asset-referenced token", "e-money token", "crypto-asset service provider" and "white paper" define the legal regime of issuance, disclosure of information, authorization, supervision and protection of investors[26]. Without these definitions, crypto-assets would remain technical and economic phenomena without a clear legal qualification.

The Ukrainian context also demonstrates the need for a systematic approach to the TLN[27]. The legislation of Ukraine on information, electronic communications, electronic identification and electronic trust services, personal data protection, national informatization and future AI regulation contains a significant number of technical concepts, but often does not have a unified methodology for their transformation into full-fledged technical and legal norms.

The problem is not that such definitions are lacking at all. On the contrary, they exist in different acts, but remain fragmentary, sometimes incompatible, sometimes too narrow or too general. Digital law requires not only a set of terms, but systemic definitive-normative architecture. Examples of functional classification of such definitions are given in Table. 2.

Table 2. Classification of Technical and Legal Definitions in Digital Law

Definition Type	Object of regulation	Example	Regulatory function
Subject-oriented	Digital Entity	Digital personality, AI-agent	Attribution of rights, duties and responsibilities
Object-oriented	Digital object	Digital asset, token, digital twin	Determination of the legal regime of the object
Process-oriented	Digital Process	Automated solution	Regulation of procedure and guarantees
Risk-based	Technological risk	High-risk AI system	Launch of enhanced compliance responsibilities
Infrastructure	Digital infrastructure	Identity wallet, platform, blockchain network	Definition of the Operating Legal Environment
Evidence	Digital footprint	Log, metadata, audit trail	Supporting Proof and Accountability
Jurisdictional	Digital Legal Event	Cross-border platform action	Definition of applicable law and competence

Legislative analysis gives grounds for an important conclusion: modern digital legislation already actually uses technical and legal definitions, but is not yet sufficiently aware of the need to transform them into a TLN as an independent type of regulatory construction. It is this methodological awareness that forms the basis of the further part of the article.

4. From technical definition to technical-legal norm

To build a correct theory of TLN, it is necessary to clearly distinguish three levels: technical definition, technical-legal definition and technical-legal norm. The technical definition explains the object in the language of the corresponding technology. The technical and legal definition defines this object in legally significant features. A technical-legal norm establishes legal consequences, rules of conduct, guarantees, duties, procedures and responsibilities associated with this object.

For example, the technical description of a biometric system might include information about sensors, patterns, comparison algorithms, databases, accuracy, and error parameters. The technical-legal definition should establish what exactly is considered biometric identification for the purposes of law. The TLN must determine when such identification is allowed, who can apply it, what safeguards are required, whether consent or other legal basis is required, what audit logs must be kept, how the error is disputed, who is responsible for the damage and which authority has jurisdiction.

Thus, the logic of transformation looks like this: technological phenomenon — technical description — legally significant features — technical-legal definition — technical-legal norm — legal consequences — jurisdictional attribution. This sequence is key to the normative engineering of digital law (Fig. 2).

The biggest mistake lies in the mechanical transfer of technical documentation to the law. Technical documentation can be too detailed, unstable, and dependent on a specific manufacturer or software architecture. The law, on the contrary, should record legally significant features that retain regulatory relevance despite technological changes.

At the same time, the opposite approach is also dangerous, when the law uses too general terms without technological specifics. In this case, the norm becomes declarative and cannot be applied to real digital systems. For example, a general ban on "misuse of AI" without a definition of AI system, subject of responsibility, risks, verification procedures, and evidentiary criteria does not create an effective legal regime.

TLN must overcome both extremes. It should not be technical instruction, but it cannot be an abstract declaration either. Its task is the legal condensation of technological knowledge. It should transform technical properties into legal criteria, and legal criteria into applicable regulatory consequences.

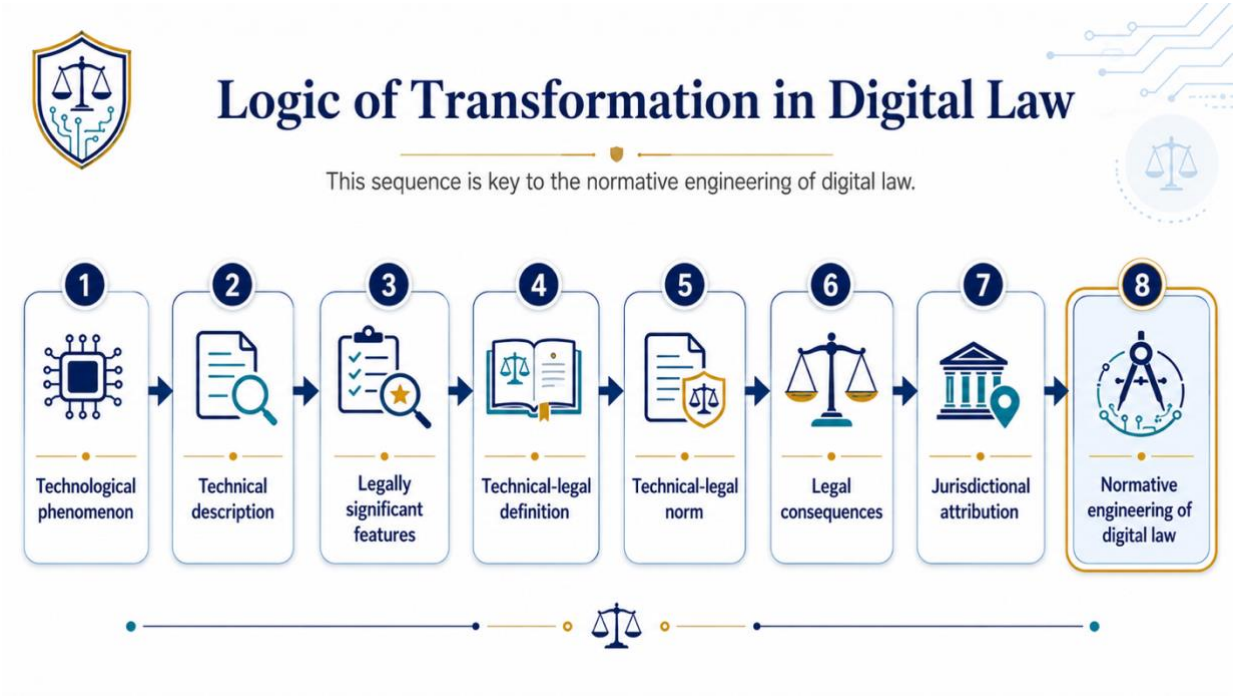


Fig. 2. *Scheme of the logic of transformation of the technical and legal definition in the TUN.*

Structurally, the TLN must contain at least the following elements: subject of regulation; subjects of rights and obligations; object or technological phenomenon; legal conditions of application; permitted and prohibited actions; documentation obligations; risk assessment procedures; human oversight mechanisms; standards of proof; audit procedure; criteria of responsibility; exceptions; update mechanism; jurisdictional reference (Fig. 3.)

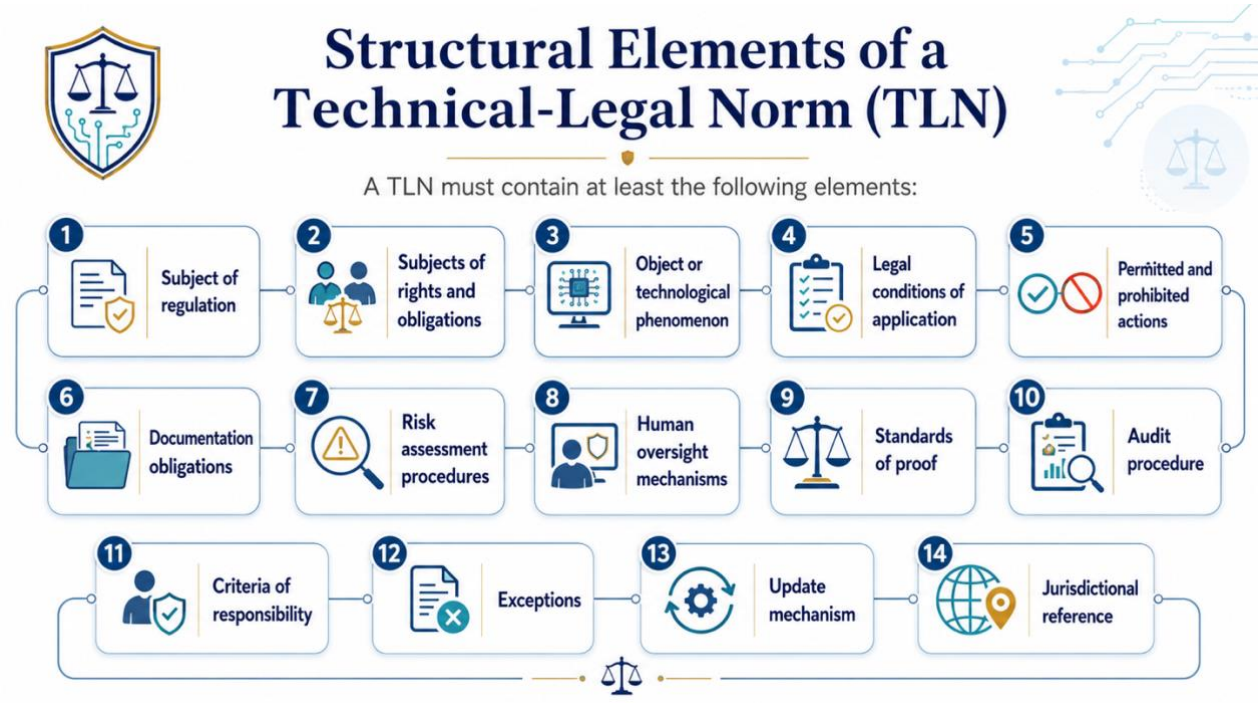


Fig. 3. *Structure of TLN*

In this sense, TLN is a real element of modern information law. Its technical component does not diminish its legal nature. On the contrary, it is the technical component that allows the norm to work in a digital environment, where legal facts arise in the form of data, logs, algorithmic results, digital traces, metadata, and automated actions.

The TLN performs at least eight functions: semantic, legal, technical, algorithmic, evidence-based, jurisdictional, interoperable and human rights. The semantic function stabilizes the meaning of the term. The legal function establishes rights, duties and responsibilities. The technical function captures the relevant characteristics of the system. The algorithmic function allows you to check the norm in digital environments. The evidentiary function determines which digital data has legal force. The jurisdictional function establishes a connection with the legal order. The interoperable function ensures compatibility between systems. The human rights function embeds guarantees against technological damage.

That is why an ordinary definition without a norm is insufficient, and a technical standard without legal transformation is not right. TLN is the point where legal normativity, technological reality and digital evidence intersect. Its place in digital jurisdiction is systematized in Table. 3.

Table 3. Technical and Legal Definitions in the Architecture of Digital Jurisdiction

Element of digital jurisdiction	Necessary technical and legal definition	Legal effect	Technical effect
Digital Entity	Digital identity, user, AI-agent	Attribution of rights and obligations	Identity recognition
Digital object	Digital assets, avatar, digital twin	Definition of ownership, use, liability	Object classification
Digital Action	Automated decision, transaction, moderation act	Creating a legal effect	Fixing an event
Digital environment	Platform, Metaverse space, blockchain network	Determination of the mode of application	System boundaries
Proof	Log, metadata, audit record	Confirmation of violation or compliance	Traceability
Responsibility	Provider, deployer, operator	Division of responsibility	Role mapping
Jurisdiction	Digital legal event	Applicable law and competent authority	Cross-border communication

5. Model Algorithm for Designing Technical and Legal Norms

The central result of the article is the algorithm for designing TLN using AI-assisted legal modelling under mandatory human supervision. This algorithm does not provide for the replacement of a legislator or lawyer with artificial intelligence. Its purpose is to use AI as an analytical, comparative, editorial, test, and revision tool, leaving the final regulatory decision up to humans.

The algorithm assumes that AI can be trained on arrays of national legislation, EU law, international documents, case law, technical standards, model laws, and doctrinal sources. However, even the most advanced AI system lacks democratic legitimacy, a constitutional mandate, ethical responsibility, or the ability to independently determine the public interest. Therefore, the model must be AI-assisted, but human-controlled.

The general structure of the ten-step algorithm is presented in Table. 4.

Table 4. Algorithm of ten stages of designing technical and legal norms

Stage	Function AI	Human Expert Function	Result
1. Identification	Search and mapping of legal sources	Determination of the legal relevance of the phenomenon	Legal relevance map
2. Technical analysis	Highlighting technical characteristics	Selection of legally significant features	Matrix "technique — law"
3. Benchmarking	Comparison of jurisdictions and definitions	Evaluating the compatibility of models	Comparison table
4. Definition of signs	Ranking of legal features	Approval of the normative model	Model Sign
5. Alternative definitions	Generation of a narrow, broad and functional definition	Selection or combination of options	Definition package
6. Transformation into normal	Preparation of the structure of the TLN	Verification of legal normativity	TLN Project
7. Justification	Formation of legal, risk, rights rationale	Doctrinal and constitutional verification	Explanatory note
8. Approbation	Generation of test cases	Assessment of fairness and applicability	Approbation report
9. Revision	Identification of collisions, gaps, duplications	Final legal version	Corrected TLN
10. Publication and monitoring	Tracking changes in law and technology	Decision to change or retain	Current or model TLN

Further, each stage is disclosed in detail, defining the purpose, the role of AI, the role of a human expert, the expected result, risks, and the connection with digital law and digital jurisdiction.

Step 1. Identification of a technological phenomenon that requires legal regulation

In the first stage, it is necessary to identify the technological object, process or digital action that acquires legal significance. It can be an artificial intelligence system, an AI-agent, a digital avatar, a digital identity, a digital identity wallet, a biometric system, a smart contract, a digital twin, a recommendation system, a tokenized asset, a standalone platform, or an event in a Metaverse/Web 4.0 environment[28].

AI should carry out a search and primary mapping of national, European and international legislation to discover whether the relevant phenomenon is mentioned directly, indirectly or through related concepts. It can quickly determine whether there are legal definitions, case law, regulatory guidelines, standards, or draft laws that address such a phenomenon.

At this stage, a human expert determines whether the phenomenon is an independent object of legal regulation, or only a technical characteristic of an already known legal institution. For example, not every algorithm needs a separate law, but the algorithm that makes decisions about access to a service, credit, education, or public assistance acquires legal significance.

The expected result is a primary map of the legal relevance of a technological phenomenon. The risk is either premature regulation of a purely technical detail or ignoring a phenomenon that already actually affects human rights, the market, public administration or digital jurisdiction.

Step 2. Technical analysis of the phenomenon without direct copying of technical documentation

The second stage is aimed at understanding the technological nature of the phenomenon. At this level, technical standards, documentation, system architecture, technology lifecycle, functions, limitations, risks, vulnerabilities, data types, control mechanisms and the role of a person in the system are analyzed.

AI can extract key functional characteristics from technical sources: autonomy, adaptability, data dependency, types of input and output data, explainability, traceability, cybersecurity, interoperability, auditability, the presence of human-in-the-loop or human-on-the-loop mechanisms.

A human expert must separate technical features that have legal significance from purely engineering details. The law should not duplicate the manufacturer's documentation. It must establish those characteristics that affect the rights, obligations, evidence, risks, responsibilities and competence of the authorities.

The expected result is the table "technical characteristics — legal relevance". It is on this basis that the future technical and legal definition is formed. The risk is the mechanical transfer of technical language into the law or, conversely, the removal of critical technological features from the norm.

Step 3. Comparative analysis of definitions and norms in different jurisdictions

The third stage involves a comparison of how the relevant phenomenon is defined or regulated in the law of the EU, the United States, the United Kingdom, Canada, China, Ukraine, international organizations and model documents. Comparative analysis is needed not for mechanical borrowing, but for the identification of regulatory patterns.

AI can compare dozens of regulations, find common elements, identify discrepancies, mark definitive gaps, excessively broad or excessively narrow wording. It can prepare a matrix: jurisdiction — definition — technical element — legal consequence — weak point.

A human expert assesses the compatibility of foreign models with national law. For example, the Chinese model may be effective for centralized state control, but unsuitable for a legal system that is based on the rule of law, proportionality, privacy protection, and judicial review. The European model may be the closest for Ukraine, but it also needs to be adapted.

The expected result is a comparative matrix of technical and legal definitions and norms. The risk is non-critical legal transplantation. TLN must be harmonized with international approaches, but cannot be a simple translation of a foreign act.

Step 4. Determination of legally significant features of a technological phenomenon

The fourth stage is filtering. After analyzing technical and legal sources, it is necessary to single out not all the features of the technology, but only those that have regulatory significance. It is these signs that will become the basis of the future definition and norm.

AI can suggest a list of features and rank them by legal significance. For an AI system, these can be autonomy, adaptability, inference, impact on a person, risk to rights and freedoms, the ability to explain, logging, auditing, human control, and communication with a specific subject of responsibility.

The human expert must approve the final system of signs. It determines which characteristics are necessary for legal qualification and which can be left in regulations, technical standards or documentation. This is where technical knowledge is transformed into legal relevance.

The expected result is the normative model of features. The risk is excessive technicality, which will make the norm unstable, or excessive abstractness, which will make it unusable.

Step 5. Designing at least three alternative technical-legal definitions

The fifth stage is to create several definitions. Digital law should not adopt the first proposed wording. For a complex technological phenomenon, at least three options are required: narrow, wide and functional.

AI generates variations of definitions explaining the advantages, disadvantages, and scope. The narrow definition provides high accuracy and is suitable for high-risk or sectoral regulation but may not cover future modifications to the technology. A broad definition is flexible but can create excessive regulatory coverage. A functional definition defines a phenomenon through functions, legal consequences and risks, therefore it is most suitable for digital law, although it requires additional enforcement criteria.

An expert compares options and chooses the basic ones. A combined definition that combines a functional approach with minimal technical criteria is often optimal. At this stage that a balance between technological neutrality and legal certainty is formed.

The expected result is a package of alternative technical and legal definitions with justification. The risk is to adopt a definition that is either too narrow and will quickly become obsolete, or too broad and create unwarranted interference with digital innovation.

Step 6. Transformation of a definition into a technical and legal norm

The sixth stage is central. It is here that the definition ceases to be a terminological element and turns into a normative construction. The TLN should not only explain what a technological phenomenon is, but also determine what legal consequences arise in connection with its creation, use, modification, blocking, transfer or damage.

AI can suggest the structure of the norm: subject of regulation, subjects, objects, conditions of application, permits, prohibitions, obligations, control procedures, documentation, audit, human oversight, evidence, liability, and exceptions. It can also form several editions of the norm: rigid, balanced and flexible.

An expert checks whether the text is a legal norm. If the wording only describes the functions of the system or repeats the technical documentation, it is not a TLN. The norm must contain a legal imperative, disposition, boundaries of behavior, control and consequences of the violation.

The expected result is the first TLN project. The risk is the creation of a pseudo-legal technical description without binding, without procedure, without responsibility and without the possibility of judicial or administrative application.

Step 7. Justification of the normative need for TLN

The seventh stage involves the preparation of doctrinal, human rights, regulatory and practical justification. No TLN should be created just because the technology is new. It is necessary to prove what legal gap it closes, what risk it reduces and what public interest it protects.

AI can form several blocks of rationale: legal rationale, risk rationale, human rights rationale, interoperability rationale, jurisdictional rationale. It can show which rights are affected by technology, what negative scenarios are possible, which existing regulations are insufficient and why a technical standard cannot replace the law.

The human expert strengthens the doctrinal argumentation, checks constitutionality, proportionality, compliance with the principle of legal certainty, the limits of interference with the freedom of innovation and the balance between private, public and technological interests.

The expected result is an explanatory note to TLN. The risk is regulatory inflation: the creation of many technical and legal norms without sufficient justification, which will complicate digital law instead of making it understandable.

Step 8. Approbation of the norm on model legal technological cases

The eighth stage consists in testing the TLN on realistic scenarios. The norm can be logically convincing on paper but not work in a real digital environment. Therefore, it must be tested through model cases.

AI can generate a series of test situations: AI mistakenly identifies an individual; a digital avatar concludes a transaction; the smart contract automatically writes off the asset; the digital twin is used as evidence; Metaverse platforms locks digital identity; the recommendation system manipulates user behavior; AI-agent acts beyond its authority.

A human expert assesses whether the norm gives a fair, legal, predictable and demonstrably verifiable result. It checks whether it is possible to establish the subject of responsibility, whether there is an appeal procedure, whether human rights are not violated, and whether there are sufficient guarantees of human oversight.

The expected result is an approbation report. The risk is to adopt a norm that looks right in abstraction but does not provide an answer to real digital conflicts.

Step 9. AI Audit, Human Legal Audit, and Adjustments

The ninth stage is the stage of multi-level audit. AI can check the text for internal logic, terminological consistency, possible collisions, duplications, gaps, excessive breadth, discriminatory risks, lack of guarantees, inconsistency with the EU AI Act, GDPR, DSA, Data Act, eIDAS 2.0, Cyber Resilience Act, and MiCA.

AI can also perform a stress-test: simulate non-standard cases, identify the possibility of circumventing the norm, check whether it does not create an excessive burden for small innovative actors, whether it does not leave the user without protection, or does not allow the delegation of public power to the algorithm without control.

A human expert conducts a final legal audit. It checks constitutionality, sectoral affiliation, compliance with information law, the limits of delegation to technical standards, the quality of legislative technique, legal clarity, judicial applicability and political and legal acceptability.

The expected result is a corrected version of the TLN. The risk is over-reliance on AI auditing. AI can detect formal inconsistencies, but it cannot definitively determine the fairness, legitimacy, and constitutional permissibility of a norm.

Step 10. Final publication, implementation and periodic AI-assisted monitoring

The tenth stage completes the design cycle. After adjustment, the TLN is prepared for publication, expert discussion, regulatory impact assessment, inclusion in a draft law, digital code, model act or by-law.

AI can support the publication stage: generate comparative tables, explanatory notes, compliance matrices with EU law, risk analysis, implementation scenarios, monitoring changes in legislation, judicial practice and technical standards. Once implemented, AI can track whether the norm is becoming obsolete due to technological changes.

The human expert makes the final decision to adopt, change or reject the norm. It is up to the person to determine the moment when technological renewal requires legal revision, and when it is enough to leave the norm stable to ensure legal certainty.

The expected result is a valid or model TLN with a periodic review mechanism. The risk is the technological obsolescence of the norm or, conversely, excessively frequent updates, which destroy the stability of the legal regime.

6. The role of a human expert in creating, adjusting and implementing the TLN

The participation of AI in the design of TLN cannot be considered as autonomous rulemaking. AI can analyze arrays of legislation, compare jurisdictions, identify conflicts, generate alternative formulations, and test model cases. However, it does not have democratic legitimacy, does not bear political responsibility, does not have a constitutional mandate and cannot independently determine a fair balance between human rights, public interest and innovation.

A human expert must be present at all stages of design. At the stage of identification, it determines whether a technological phenomenon requires legal regulation. At the stage of technical analysis, it selects legally relevant features. At the stage of comparative analysis, it assesses the possibility of legal adaptation of foreign models. At the stage of definitions, it chooses between a narrow, broad and functional edition. At the stage of creating a norm, it ensures its legal nature.

Of particular importance is a human expert in determining human rights guarantees. AI can suggest wording on transparency, auditing, or human oversight, but only a lawyer can assess whether such wording complies with constitutional guarantees, the principle of proportionality, due process, access to legal protection, and the prohibition of discrimination.

In a digital jurisdiction, this aspect is of fundamental importance. If the legal order recognizes the legal consequences of digital actions, algorithmic decisions or platform acts, then a person should be able to appeal against such actions, receive explanations, identify the responsible entity and demand the restoration of the violated right. The TLN must be designed so that digital automation does not turn into irresponsible algorithmic power.

Human control is also needed to prevent regulatory dependence on private technology standards. If the law too directly delegates legal significance to technical specifications, private developers or standardization organizations can influence the content of rights and obligations. TLN should consider the standards but not replace the law with them.

Therefore, AI in the design of TLN should have the status of an intelligent tool, and not a source of regulatory power. A person remains the bearer of legal responsibility for the final text, its value orientation, constitutional admissibility and practical justice.

7. TLN as the definitive core of digital law and digital jurisdiction

Digital jurisdiction requires more than just a procedural or institutional description. It requires a definitive core that allows the law to recognize digital subjects, digital objects, digital actions, digital evidence, and digital environments. Without such a core, digital jurisdiction remains a declaration, since the law enforcement does not have stable criteria for the qualification of digital phenomena.

The basic categories of the definitive core of digital law include: digital subject, digital identity, digital identity, digital avatar, AI-agent, digital twin, digital object, digital asset, tokenized asset, platform rule, smart contract, automated decision, digital proof, digital legal event, algorithmic act, and human oversight mechanism (Table 5).

Table 5. Matrix for assessing the quality of a technical and legal norm

Criterion	Questions to check	A sign of high-quality TLN
Legal certainty	Is it clear when the norm is applied?	Clear conditions of application
Technological correctness	Does the norm distort the technological nature of the phenomenon?	Essential technical characteristics are taken into account
Human rights	Does the norm contain human rights guarantees?	Transparency, appeal, human oversight are provided
Evidence	Is it possible to prove compliance or violation of the norm?	Logs, metadata, audit trail defined
Jurisdiction	Is it clear which legal order is competent?	There are criteria for digital binding
Interoperability	Is the norm compatible with other systems and modes?	Cross-border and standards are taken into account
Adaptability	Can the norm survive technological changes?	There is a mechanism for viewing without losing stability

Each of these categories requires not only a definition, but also a TLN. For example, the definition of a digital avatar alone does not resolve the question of whether an avatar can represent a person, enter transactions, have reputational attributes, be blocked, modified, inherited, or used as evidence. This requires a technical and legal norm.

Similarly, a digital twin cannot be regulated only as a "digital representation of a physical object". The law must determine whether a digital twin can be proof of the state of a physical object, who is responsible for its accuracy, how the moment of updating is recorded, what consequences an error has, whether it can be the subject of a transaction and whether it is subject to jurisdictional recognition in a cross-border environment.

A smart contract also needs a TLN. A technical code can automatically fulfill a condition, but the law must determine whether such an action is a legal act, who is responsible for the error of the code, how to appeal against automatic execution, whether suspension of execution is allowed, what evidence confirms the will of the parties, and which court has jurisdiction.

Thus, digital jurisdiction is not built directly from technology. It is built from technical and legal norms that transform technological actions into legally cognizable structures. This means that TLN is not an optional element of digital law, but its definitive-normative core.

This approach is consistent with the idea of digital code. A digital code cannot be a simple collection of norms about AI, data, platforms, blockchain, and Metaverse. It should be a modular normative architecture in which each digital phenomenon receives a definition, norm, procedure, guarantee, evidentiary regime, responsibility and jurisdictional connection.

The proposed model of the definitive core has eight levels: semantic, legal, technical, algorithmic, jurisdictional, evidence-based, human rights and interoperable. The semantic level determines the meaning of the term. The legal level establishes rights and obligations. The technical level captures the relevant characteristics. The algorithmic layer provides the possibility of automated verification. The jurisdictional level determines the competent legal order. The evidentiary level establishes significant digital traces. The human rights level embeds guarantees. The interoperability layer ensures compatibility between systems and jurisdictions.

8. TLN Application Modules: AI-agent, Digital Avatar, Digital Twin, Recommendation System, Smart Contract, and Digital Proof

To test the practical suitability of the proposed concept, it is advisable to consider several application modules. The first is the AI-agent. Technically, an AI-agent can be a system capable of autonomously planning actions, interacting with the digital environment and achieving its goal. However, such a description is not enough for law. The TLN must determine who authorizes the agent, what are the limits of his action, what are the legal consequences of going beyond authorization, whether the agent can enter into transactions, who is responsible for the error, and what logs confirm his behavior.

The second module is a digital avatar. In Metaverse environments, an avatar can be a human interface, an independent digital representation, a commercial image, an influencer, a bot, or a synthetic personality. The TLN should distinguish between the avatar as a visual interface, the avatar as a digital representation, the avatar

as a carrier of personal attributes, and the avatar as an object of platform control. The right to identity, reputation, blocking, modification, inheritance and protection against misuse depends on this.

The third module is a digital twin. It can reflect a physical object, a manufacturing process, a person, a city, a medical condition, or infrastructure. The legal meaning of a digital twin depends on the accuracy, data sources, frequency of updates, subject of control, evidentiary suitability and risk of error. The TLN must determine when a digital twin can be evidence, when it is only an information model, and who is responsible for the decision made based on it.

The fourth module is the recommendation system. It forms the visibility of information, influences choices, behavior, commercial decisions and political perception. The TLN should determine which systems are considered recommendatory, when they have an increased risk, what parameters should be disclosed to the user, whether there should be a right to refuse profiling, how algorithm changes are recorded, and who is responsible for the manipulative effect.

The fifth module is the smart contract. Its technical feature is the automatic execution of the code, but the legal question is whether the automatic execution corresponds to the will of the parties, whether an error is possible, whether it is possible to stop or cancel the execution, whether the code is the only proof of the conditions, and how the program code relates to the text agreement. TLN should provide a bridge between contract law and algorithmic enforcement.

The sixth module is digital proof. In a digital environment, proofs can be logs, metadata, hashes, timestamps, transaction records, digital signatures, audit logs, API records, output AI systems, and platform events. The TLN must determine which digital traces are acceptable, proper, reliable, integral and verifiable. Without this, digital jurisdiction cannot be exercised procedurally.

These examples confirm that TLNE is a universal instrument of digital law. It allows not only to describe the new technology, but also to give it a legal form, determine the boundaries of behavior, establish responsibility and provide evidence.

9. Discussion

The proposed approach changes the place of definitions in law. In classical law, definitions are often placed at the beginning of the act and are perceived as auxiliary provisions. In digital law, they become the infrastructure of regulation. The entire legal regime depends on how the AI system, digital identity wallet, recommender system, or crypto-asset is defined.

However, the main conclusion of the article is that even a technical and legal definition is no longer enough. It must be converted to TLN. Otherwise, digital law will remain at the level of terminological description and will not be able to establish effective procedures, guarantees, evidentiary standards and liability.

The advantage of the proposed algorithm is its versatility. It can be applied to AI, digital identity, platforms, Metaverse, cybersecurity, crypto assets, digital proofs, smart contracts, and digital twins. It can also be used in legislative work, expert preparation of acts, scientific modeling, regulatory sandbox and development of a digital code[29].

At the same time, there are risks. The first risk is excessive technicalization of the law. If the norm is too dependent on the specific architecture of the system, it will quickly become obsolete. The second risk is excessive abstraction. If the norm does not contain technical criteria, it will be unsuitable for application. The third risk is over-reliance on AI in rulemaking. The fourth is the privatization of regulatory content through technical standards.

To overcome these risks, the TLN should be based on the principle of legally significant technicality. This means that the norm does not include all technical details, but only those that affect rights, obligations, liabilities, evidence, risks, jurisdiction and guarantees. This approach allows you to maintain the stability of the law and at the same time ensure its ability to work with digital technologies.

For Ukraine, this methodology is of particular importance. The future Ukrainian regulation of AI, digital identity, platforms, data, and the Metaverse[30] should be shaped not only by implementing European terms, but by creating its own doctrinally based TLN system[31]. This will combine European integration, national legal tradition, information law, digital jurisdiction and the needs of innovative development.

In a broader theoretical sense, TLN can be seen as the basic unit of normative engineering of the digital age. If the XX century worked mainly with norms addressed to a person, organization or state, then the XXI century increasingly needs norms that regulate the interaction of a person, data, algorithms, platforms, digital objects and automated infrastructures.

That is why the proposed approach has not only applied, but also doctrinal significance. It shows that information law is no longer a peripheral industry that serves technology. It becomes a methodological center for the formation of legal regimes of digital civilization.

10. Additional provisions on the law-making technique of TLN

The TLN must be formulated in language that combines sufficient legal clarity with controlled technological precision. This means that it should not contain excessively variable technical parameters that are best left for by-laws or standards, but it should contain criteria without which enforcement will be impossible.

In the structure of the normative act, the TLN can perform various functions. It can be a general norm-definition, norm-regime, norm-procedure, norm-guarantee, norm-responsibility or norm-jurisdictional bridge. That is why in Table. 2 The classification of technical and legal definitions is related to the types of regulated objects and their regulatory function.

The legislator should avoid two defects: definitive minimalism and definitive maximalism. Definitive minimalism occurs when a law uses a technological term without a proper definition. Definitive maximalism arises when the law overloads the definition with technical details and replaces the legal norm with the technical passport of the system.

The optimal TLNe should be built on the principle of modularity. The basic concept is enshrined in the law; technical parameters can be detailed in a by-law or standard; procedural guarantees are enshrined in the legal regime; evidentiary requirements are defined in procedural or special legislation; The update mechanism ensures adaptation to technological dynamics.

In the field of digital jurisdiction, the TLN should also contain binding criteria: subjective, object, territorial, platform, contractual, given, infrastructural or spectacular. For example, a digital event may be related to a jurisdiction due to the user's location, the provider's place of registration, the language of the service, the target market, the location of the damage, or the technical infrastructure.

Special attention should be paid to the ratio of TLN and technical standards. The standard can perform an auxiliary function but should not independently determine the scope of rights and obligations. The law may refer to the standard to prove compliance, but the key legal consequences should remain in the law.

TLN must also be compatible with the principle of technological neutrality. This means that the norm should not regulate a specific technology as a product, but a legally significant function, risk or consequence. This approach allows you to apply the norm to future technological forms that perform a similar function.

At the same time, technological neutrality should not turn into technological blindness. If certain characteristics, such as real-time biometric identification or autonomous decision-making, pose a particular risk, the law should explicitly record them as legally significant features.

Thus, the legislative technique of the TLN should be based on a balance between stability and adaptability, between legal language and technological precision, between man and algorithm, between national law and cross-border interoperability.

11. Model structure of the technical and legal norm as an article of the future digital code

For practical use of the proposed concept, it is advisable to show how exactly the TLN can be formalized in the structure of the future digital code or a special law on digital technologies. Such a norm should consist not of one sentence definition, but of a sequential set of normative elements. The first element is definitive: it defines the object of regulation in legally significant technical features. The second element is subjective: it establishes who is the provider, developer, operator, user, deployer, controller, platform operator or other bearer of responsibilities. The third element is functional: it describes what actions or functions of technology create legal consequences. The fourth element is guarantee: it enshrines transparency, explainability, the right to information, the right to appeal and human control.

The fifth element of the TLN is procedural. It specifies what steps the subject must take before using the technology: risk assessment, documentation, registration, notification of the user, testing, audit, consultation with the supervisory authority or carrying out impact assessment. The sixth element is evidence. It specifies which digital traces, logs, metadata, audit trails, hashes, timestamps, or output records should be stored to confirm the legitimacy of the action. The seventh element is responsibility. It establishes who is responsible for an error, damage, illegal data processing, discriminatory result, unauthorized action of an agent or a defect in a digital object.

The eighth element is jurisdiction. It fixes the criteria by which a digital action or a digital object is tied to a certain legal order. For digital law, this is especially important, since a technological action can be created in one state, performed on a server in another, affect the user in a third, and have legal consequences in a fourth. The TLN must provide for the following linking criteria: the place of destination of the service, the place of occurrence of the damage, the location of the data subject, the place of the main establishment of the provider, the market to which the service is directed, or the digital environment in which the event occurred.

The ninth element is the renewal mechanism. TLN cannot be a frozen norm if it regulates rapidly changing technologies. However, the update should not destroy legal certainty. Therefore, the law may provide for periodic audits, regulatory guidelines, sandbox mechanisms, delegated technical annexes or AI-assisted monitoring. The tenth element is the limits of delegation to technical standards. TLN should clearly establish which issues can be detailed by the standards, and which remain exclusively in the field of law. Rights, obligations, responsibilities and fundamental guarantees should not be consigned to the level of a private technical specification.

In this sense, TLN is not just a formula or definition. It is a small regulatory module that can be included in a large digital code system. If the classic article of the law often contains a hypothesis, a disposition and a sanction, then the TLN in digital law has an extended structure: definition, technical criteria, subjects, functional boundaries, procedures, guarantees, evidence, liability, jurisdiction and updates. This structure corresponds to the complexity of digital environments and allows the law to keep up with technological practices.

The model TLN for AI-agent could contain the following logic: AI-agent is a digital system that, based on the prior authorization of the subject, is able to autonomously or semi-autonomously form actions in the digital environment to achieve a certain goal. The use of AI-agent is allowed only if the boundaries of authority, the subject of responsibility, logging of actions, the possibility of suspension, human control and the procedure for appealing the result are determined. The actions of an AI-agent cannot create legal consequences for the user if they have gone beyond the confirmed authorization or have been carried out without proper identification of the entity responsible.

A model TLN for a digital avatar could proceed from the fact that the avatar is a digital representation of a person or an autonomous digital image used in the digital environment for communication, representation, interaction or commercial activity. The norm should distinguish between an avatar as an interface and an avatar as a legally significant representation. In the second case, the rules of identification, consent, boundaries of representation, protection of reputation, prohibition of unlawful copying, protection against deepfake imitation, and the right to restore access after blocking are necessary.

A model TLN for a digital twin should record that a digital twin is a dynamic digital model of a physical, biological, social or infrastructural object, which is based on data and can be used for analysis, forecasting, management or proof. The legal significance of a digital twin depends on the data sources, the frequency of updates, verification methods, the level of accuracy, the subject of control and the procedure for appealing an erroneous result. Without these elements, the digital twin cannot have full evidentiary value.

A model TLN for a recommendation system should define it as an automated or semi-automated system that selects, ranks, prioritizes or offers information to the user based on data, profiling, context, behavior or commercial parameters. The norm should provide for the transparency of the main parameters, the user's right to an alternative mode without profiling in certain cases, the audit of manipulative effects, the protection of minors and the responsibility of the platform for covert discrimination or systemic manipulation.

A model TLN for digital proof should define digital proof as data, metadata, log, transaction record, hash, electronic signature, timestamp or other digital trace that can confirm a legally significant circumstance, subject to integrity, authenticity, traceability and verifiability. Such a rule should determine who keeps the evidence, how its immutability is ensured, how its origin is verified, who has access, how the reliability is challenged and what standard of proof is applied.

Thus, the practical model of the TLN shows that digital law should not remain at the level of general declarations. It must learn how to create norms that simultaneously work for a lawyer, judge, regulator, developer, auditor and user. This is what turns TLN into a real tool for the legal organization of digital civilization.

12. Variability of Definitive Design: Narrow, Broad and Functional Model

A separate element of the methodology is the variability of definitive design. For each complex technological phenomenon, it is necessary to create not one, but at least three definitive models. This is necessary because different regulatory purposes require different breadths of concept. High-risk regulation requires precision; innovative regulation requires flexibility; Digital jurisdiction requires a functional link to legal consequences.

A narrow definition is suitable for cases where the law must cover a specific risk. For example, when it comes to real-time biometric identification in public space, the definition should be clear enough not to cover every form of video analytics, but at the same time does not allow the ban to be circumvented by changing the name of the technology. A narrow definition reduces uncertainty but can quickly become obsolete or leave out of regulation functionally similar systems.

A broad definition is useful where technology is changing rapidly, and the law must have future applicability. For example, a broad definition of a digital object can include virtual objects, tokenized assets, digital twins, game objects, avatars, synthetic media, and other forms that do not yet have an established legal regime. The risk of a broad definition lies in excessive coverage and creation of legal uncertainty for innovative actors.

The functional definition is the most promising for digital law. It defines a phenomenon not through specific technology, but through function, influence and legal consequences. For example, an AI-agent can be defined not by a specific machine learning model, but by the ability to act autonomously in the digital environment in the interests or on behalf of the subject. This definition is more resistant to technological changes but requires additional application criteria.

AI can effectively assist in the creation of three definitions. It can model which objects will fall under a narrow definition, which will fall under a broad definition, and which will fall under a functional one. It can also show the risks of over-inclusion and under-inclusion. However, the choice of the final model must be made by an expert person, since it is not only a technical, but also political and legal one.

In the context of digital jurisdictions, functional definition often takes precedence. Digital jurisdiction is interested not only in the nature of technology, but primarily in what legal consequences it creates: who acts, where the effect occurs, who controls the system, who benefits, who suffers harm, and what legal order has competence. Therefore, the functional definition better combines law and technology.

At the same time, in high-risk areas — biometrics, critical infrastructure, medical AI, law enforcement systems, automated access to social rights — it is advisable to combine a functional definition with specific technical features. This avoids excessive abstraction and ensures the controllability of law enforcement.

Therefore, the variability of definitive design is not an editorial exercise, but a necessary stage of normative engineering. It allows you to see the consequences of different formulations before the adoption of the norm, reduce the risk of regulatory error and ensure a higher quality of digital legislation.

13. Criteria for approbation and revision of the TLN in law enforcement practice

Approbation of the TLN should not be formal, but scripted. This means that the norm is checked not only for compliance with legal technique, but also for the ability to resolve real legal technological conflicts. Such verification shall include normal scenarios, boundary scenarios, abuse scenarios, error scenarios, cross-border effect scenarios and human rights violation scenarios.

The first criterion for approbation is applicability. The norm should answer the question of whether it can really be applied to a digital event. If the law enforcement officer cannot establish whether the system falls under the norm, who is the responsible entity and what evidence is needed, such a TLN is of poor quality. The quality norm must have a clear applicability threshold.

The second criterion is evidence. Digital law cannot exist without digital evidence. If TLN establishes an obligation, but does not specify which logs, records, metadata, or audit trails confirm its completion, it remains declarative. Therefore, each TLN must contain either directly or through an adjacent norm an evidentiary mechanism.

The third criterion is subjective certainty. In digital systems, developer, provider, deployer, user, data controller, processor, platform operator, third-party integrator, and AI-agent often operate. TLN should distribute responsibility between these roles. Otherwise, a situation of responsibility arises without a responsible subject.

The fourth criterion is human rights sufficiency. The norm should ensure the protection of privacy, dignity, non-discrimination, autonomy, access to information, the right to appeal and the right to an effective

remedy. If the TLN regulates a technology that affects a person, it must contain not only the responsibilities of the operator, but also the procedural capabilities of the user.

The fifth criterion is jurisdictional suitability. If digital action is of a cross-border nature, the norm should make it possible to establish which legal order has competence. This requires criteria for the direction of the service, the effect, the place of damage, the location of the user, the place of establishment of the provider or other relevant communication.

The sixth criterion is technological resilience. The TLN should not become obsolete due to changes in the software product version. It must regulate a legally significant function, risk, or consequence. Technical details may be updated through standards or subordinate regulations, but the legal framework itself should remain stable.

The seventh criterion is compatibility with other modes. TLN must comply with the rules on personal data, cybersecurity, electronic identification, consumer protection, competition, administrative law, civil liability and procedural evidence. AI can help identify collisions, but the final assessment belongs to a human expert.

The eighth criterion is auditing. A high-quality TLN should contain or provide for a revision mechanism. This can be a periodic audit, regulatory review, sunset clause, the regulator's obligation to publish guidance, or AI-assisted monitoring of changes in technical standards and application practices. Without auditing, digital law risks becoming obsolete faster than it will be applied.

Therefore, the approbation and revision of the TLN is not the final formal stage, but a necessary mechanism for ensuring the quality of digital legislation. It is through testing, revision and adjustment that the TLN turns from a theoretical structure into a real tool of information law.

14. Conclusions

The study substantiates technical and legal definitions as initial modules of modern digital law and proves the need for their further transformation into technical and legal norms — a new type of normative construction of information law.

It has been established that the usual legal definition is not able to fully ensure the regulation of complex digital phenomena. It can stabilize the term, but it is not always able to reflect technological functionality, algorithmic implications, evidentiary suitability, interoperability, and jurisdictional linkage.

It has been proved that the technical-legal definition has a hybrid nature. It combines legal accuracy, technological correctness, regulatory operability, machine readability, evidentiary relevance and the ability to be included in a digital code.

It is shown that modern digital legislation uses technical and legal definitions. The EU AI Act, GDPR, Digital Services Act, Data Act, eIDAS 2.0, Cyber Resilience Act, and MiCA demonstrate that definitions of digital phenomena define not only terms, but also the boundaries of rights, obligations, liabilities, risks, compliance, and jurisdiction.

The concept of TLN as a new type of normative construction is proposed. TLN is not a copy of technical standard or software documentation. It is a legally transformed norm that transforms a technological phenomenon into a legal object with defined subjects, rights, obligations, procedures, guarantees, evidence, responsibilities and a review mechanism.

A ten-stage AI-assisted and human-controlled algorithm for the design of TLN has been developed: identification of the phenomenon; technical analysis; comparative analysis; determination of legally significant features; design of three definitions; transformation of the definition into the norm; justification of the normative need; approbation on model cases; AI audit and human legal audit; publication, implementation and monitoring.

It has been determined that AI can support the creation of TLNs but cannot replace humans. AI can analyze legislation, compare jurisdictions, generate options, test cases, and identify collisions. However, a human expert must make final decisions on values, constitutionality, proportionality, human rights, legal responsibility and public interest.

The connection of the TLN with digital jurisdiction is substantiated. A digital jurisdiction needs a definitive core to recognize digital actors, digital objects, digital actions, algorithmic decisions, platform events, and digital proofs. Without TLN, digital jurisdiction cannot be stable, evidentiary and enforceable.

The theoretical contribution of the article is to rethink definitions as initial modules of technical and legal norms. The practical value lies in the proposed algorithm, which can be used by legislators, regulators, scientists, AI governance experts, digital code developers, and information law specialists.

It is advisable to direct further research to test the algorithm for specific categories: AI-agent, digital avatar, digital identity, digital twin, smart contract, recommender system, biometric identification system, digital evidence, and Metaverse platform rule[32].

Funding: This study did not receive specific funding from public, for-profit or non-profit institutions.
Declaration of competing interest: the author declares that there is no conflict of interest.
Data availability: empirical datasets within the study were not created or analyzed.

REFERENCES

[1] Provalinsky, D. (2024). Uncertainty of the Legal Categoral Apparatus in the Field of Legal Regulation of Digital Legal Relations. *Rossijskoe pravosudie*. https://doi.org/10.37399/issn2072-909x.2025.1.5-16.

[2] Ennan, R. (2024). Digitalization of Law and formation of Digital Law. *Uzhhorod National University Herald. Series: Law*. https://doi.org/10.24144/2307-3322.2024.83.1.29.

[3] Turner, B., & Wiber, M. (2022). Legal Pluralism and Science and Technology Studies: Exploring Sources of the Legal Pluriverse. *Science, Technology, & Human Values, 48*, 457 - 474. https://doi.org/10.1177/01622439211069659.

[4] Dogaru, L. (2025). DISCUSSION ON LEGAL NORMATIVITY AND LEGAL LANGUAGE. *Curentul Juridic/Juridical Current*. https://doi.org/10.62838/cjjc-2024-0038.

[5] Veronese, A. (2025). Cultural and legal hybridism: in search of a new legal theory for the regulation of informational phenomena. *UNIO – EU Law Journal*. https://doi.org/10.21814/unio.11.1.6634.

[6] Whalen, R. (2022). Defining legal technology and its implications. *Int. J. Law Inf. Technol., 30*, 47-67. https://doi.org/10.1093/ijlit/eaac005.

[7] Sunyaev, A., Benlian, A., Pfeiffer, J., Jussupow, E., Thiebes, S., Maedche, A., & Gawlitza, J. (2025). High-Risk Artificial Intelligence. *Business & Information Systems Engineering, 67*, 981 - 994. https://doi.org/10.1007/s12599-025-00942-6.

[8] Kaltheuner, F., & Bietti, E. (2018). Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR. *, 2*. https://doi.org/10.21039/irpandp.v2i2.45.

[9] Simeonova, I. (2025). HOW GDPR TREATS AUTOMATED DECISION-MAKING. *Journal Scientific and Applied Research*. https://doi.org/10.46687/jsar.v28i1.435.

[10] Naudts, L., Helberger, N., Veale, M., & Sax, M. (2025). A Right to Constructive Optimization: A Public Interest Approach to Recommender Systems in the Digital Services Act. *Journal of Consumer Policy, 48*, 269 - 296. https://doi.org/10.1007/s10603-025-09586-1.

[11] Messmer, A., & Degeling, M. (2023). Auditing Recommender Systems - Putting the DSA into practice with a risk-scenario-based approach. *ArXiv, abs/2302.04556*. https://doi.org/10.48550/arxiv.2302.04556.

[12] Fabbri, M. (2023). Self-determination through explanation: an ethical perspective on the implementation of the transparency requirements for recommender systems set by the Digital Services Act of the European Union. *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*. https://doi.org/10.1145/3600211.3604717.

[13] Solarova, S., Mesarcík, M., Pecher, B., & Srba, I. (2026). Beyond the Checkbox: Strengthening DSA Compliance Through Social Media Algorithmic Auditing. *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3772318.3791774.

[14] Fabbri, M., & Boratto, L. (2025). Auditing Recommender Systems for User Empowerment in Very Large Online Platforms under the Digital Services Act. *Proceedings of the Nineteenth ACM Conference on Recommender Systems*. https://doi.org/10.1145/3705328.3748074.

[15] Söderlund, K., Engström, E., Haresamudram, K., Larsson, S., & Strimling, P. (2024). Regulating high-reach AI: On transparency directions in the Digital Services Act. *Internet Policy Rev., 13*. https://doi.org/10.14763/2024.1.1746.

[16] Van Roijen, D. (2024). The European Digital Identity Wallet: A Healthcare Perspective. *Blockchain in Healthcare Today, 7*. https://doi.org/10.30953/bhty.v7.344.

[17] Fernández, R. (2024). Regulatory options for integrating zero-knowledge proofs into the European Digital Identity Wallet. *International Review of Law, Computers & Technology, 39*, 303 - 326. https://doi.org/10.1080/13600869.2024.2398915.

[18] Lepore, C., Laborde, R., & Eynard, J. (2024). Aligning eIDAS and Trust Over IP: A Mapping Approach. *Proceedings of the 19th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3664476.3670919.

[19] Macan, S. (2021). Legal Acceptability of the Security Level of the Electronic Identification System. *Yearbook of the Faculty of Legal Sciences - APEIRON* . https://doi.org/10.7251/gfp2111186m.

[20] Marco, G., Marino, F., & Maria, A. (2024). Bridging eIDAS 2.0 Legal Requirements and Technical Solutions. , 18-30.

[21] Chiara, P. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review, 3*, 255-272. https://doi.org/10.1365/s43439-022-00067-6.

[22] Kamara, I. (2024). European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. *Innovation: The European Journal of Social Science Research, 37*, 1441 - 1460. https://doi.org/10.1080/13511610.2024.2349626.

[23] Ruohonen, J., Hjerppe, K., & Kang, E. (2025). A Mapping Analysis of Requirements Between the CRA and the GDPR. *2025 IEEE 33rd International Requirements Engineering Conference Workshops (REW)*, 215-222. https://doi.org/10.1109/rew66121.2025.00034.

[24] Simola, J., Takala, A., Lehkonen, R., Frantti, T., & Savola, R. (2024). Impact of Cyber Security Operations on Hardware Requirements for Stable and Workable Industrial Environments. *International Conference on Cyber Warfare and Security*. https://doi.org/10.34190/iccws.19.1.2003.

[25] Zetzsche, D., Annunziata, F., Arner, D., & Buckley, R. (2020). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal*. https://doi.org/10.2139/ssrn.3725395.

[26] Hobza, M., & Vondráčková, A. (2021). Crypto-Asset Services under the Draft MiCA Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3984355.

[27] Habibulloh, M. (2025). Digital Governance And The Right To Privacy: A Comparative Analysis Of AI Regulation In Southeast Asia And The European Union. *Journal of Law, Policy and Global Development*. https://doi.org/10.71305/jlpgd.v1i1.333.

[28] Kostenko, O. (2025). Digital Jurisdiction. Metaverse Science, Society and Law, 1(2). DOI: 10.69635/mssl.2025.1.2.23

[29] Lessig, L. (1999). Code and Other Laws of Cyberspace. Basic Books.

[30] Kostenko, O., Dniprov, O., Zhuravlov, D., et al. (2025). A New Paradigm of Metaverse Philosophy: From Anthropocentrism to Metasubjectivity. Philosophies, 10(6), 117.

[31] Kostenko, O., & Zhuravlov, D. (2025). Reconceptualizing jurisdiction and legal identity in the Metaverse: Elements of a digital code architecture. Metaverse Science, Society and Law, 1(1). DOI: 10.69635/mssl.2025.1.1.13.

[32] Kostenko, O. (2025). AI Law Model for Ethical Legislation: Strategic Recommendations for the Regulation of Artificial Intelligence. SciFormat Publishing Inc. DOI: 10.69635/978-1-0690482-5-7.