ASEJ ISSN: 2543-9103 ISSN: 2543-411X (online)

# Legal Personhood of Artificial Intelligence: From the "Punctuated Equilibrium" of Doctrine to a Non-Mimetic System of AI Legal Subjects
## (AI Legal Entity, AI Representative, AI Digital Human)

Oleksii Kostenko[1] Nataliia Onyshchenko[2], Dmytro Zhuravlov[3] and Oleh Burdeinyi[4]

[1] State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine" *Kyiv, Ukraine,*

[2] V. M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine; National Academy of Legal Sciences of Ukraine. *Kyiv, Ukraine,*

[3] Honored Jurist of Ukraine *Kyiv, Ukraine,*

[4] Originator of the project idea to establish the international scientific and practical cluster 'SHIELD (Scientific Hub for Integrity and Economic Law Defense)'

***Abstract*— The article addresses the legal personhood of artificial intelligence (AI) systems in the context of the spread of agentic systems, digital twins and metaverse environments. The aim of the study is to combine an explanatory model of the development of the debate on AI as a legal person with a constructive model of the legal status of AI subjects suitable for legislative enactment. At the first stage, the study by C. Novelli, L. Floridi, G. Sartor and G. Teubner is analysed, which describes the debate as a "punctuated equilibrium": long periods of stability are interrupted by rapid paradigm shifts driven by the competition between the singularist and cluster conceptions of legal personhood, the state of technology and AI's participation in socio-digital institutions, while the depth of the shifts is modulated by the consistency of adjacent legal regimes and by case law. The liability regimes proposed by the foreign colleagues for digital assistance, hybridity and the interconnectivity of algorithms, together with their forecast regarding AI agents and digital twins, are reconstructed. At the second stage, the concept of the AI digital human is set out, distinguishing Module 1 (Digiperson — a digital reflection of a specific natural person) from Module 2 (an autonomous Digihuman without a prototype), together with the Digital Humans Registry, the non-simulacrum principle and the right to non-algorithmic existence. At the third stage, a system of AI legal subjects of the Metaverse is proposed, built on the principle of non-mimeticity: a subject is defined not by its likeness to a human being but by its registered function and verified level of autonomy. The system comprises a status branch (the AI legal entity with three autonomy classes) and a representative branch (nine types of AI representative), an original catalogue of rights with four absolute limits, a three-dimensional registration profile, a reserve ratio, an identity anchor with status passporting, a deferred settlement finality window and a six-tier liability cascade. The methodology comprises the formal-dogmatic, comparative-legal and functional comparative methods, legal modelling and the operationalisation of technical features of autonomy on the basis of ISO/IEC 42001, IEEE 7001-2021 and the NIST AI RMF. Proposals are formulated for the draft Law "On Artificial Intelligence" concerning a single chapter on delegated digital legal personhood covering the AI legal entity, the AI representative and the AI digital human.**

***Keywords*— legal personhood of artificial intelligence; AI legal entity; AI representative; AI digital human (Digihuman, Digiperson); principle of non-mimeticity; cluster conception of legal personhood; Metaverse**

## I. INTRODUCTION

Between 2023 and 2026, generative and agentic artificial intelligence (AI) systems ceased to be mere analytical tools: they conclude transactions, conduct negotiations, dispose of digital assets, prepare draft administrative decisions and act on behalf of users in Metaverse environments in the form of an avatar or a digital twin. At the same time, the law largely continues to operate with the binary scheme of "subject — object", within which an autonomous system is classified as a software tool of the user or the operator. Three structural defects follow: non-identifiability (an injured party has no starting point from which to establish who is answerable), non-portability (an agent operating in several environments is subject to a different legal regime in each of them) and the lack of security for claims (the agent's assets are neither segregated nor available for enforcement).

The debate on the legal personhood of AI has a history of more than half a century (Solum, 1992; Chesterman, 2020; Kurki, 2019), yet its present state is contradictory. On the one hand, the European Parliament's 2017 Resolution on "electronic personhood" (European Parliament, 2017) was never implemented, and the EU "regulatory triad" — Regulation (EU) 2024/1689 (Regulation (EU) 2024/1689, 2024), the new Directive on liability for defective products

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 30 No 3 (2026) pages 14
ttps://doi.org/10.19192/wsfip.sj3.2026.1
Received: May 2026 Accepted: September 2026
Published: Septemeber 2026

Copyright: © 2026 by the authors. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial CC BY-NC 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/).
Publisher's Note: ANSBB stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

(Directive (EU) 2024/2853, 2024) and the withdrawn proposal for an AI liability directive — has entrenched the approach that "AI is a product". On the other hand, agentic systems already perform in practice roles that previously required the status of a person, and the pressure on the law is growing.

Regulatory practice in 2026 shows that legislators and courts increasingly regulate a person's digital likeness and human-like AI systems according to their function rather than their technical nature. On 8 October 2026 the Danish Government tabled in the Folketing amendments to the Copyright Act that prohibit the dissemination of realistic digital imitations of a person's face or voice without that person's consent, including imitations of artists' performances, while leaving satire, parody and criticism permitted (Euronews, 2026). This is the first attempt in the EU to vest in individuals a proprietary right to their own "digital likeness". In the United Kingdom, a bill introduced in the House of Commons by Chi Onwurah requires a person's explicit consent to the creation of their algorithmic "digital twin" — a model of their behaviour, appearance or voice (LSE Law School, 2026). In the People's Republic of China, five authorities (CAC, NDRC, MIIT, the Ministry of Public Security and SAMR) adopted interim rules for human-like AI interaction services, in force since 15 July 2026, which provide for tiered regulation, safety obligations for providers, the protection of minors and older people, security assessment, algorithm registration and regulatory sandboxes (Science and Technology Daily, 2026); in April 2026 the CAC also published draft rules for "digital human" services requiring consent to the use of a real person's features, explicit "digital human" labelling in interactive services and prohibiting the fostering of dependency among minors. In typical cases, the Beijing Higher People's Court recognised original images of virtual humans as works of fine art protected by copyright and classified the sale of AI-generated images based on others' works as a copyright offence.

In parallel, an opposite trend is emerging — the pre-emptive prohibition of AI legal personhood. A bill introduced by Ohio State Representative Thaddeus Claggett prohibits recognising any legal personhood of AI, including the role of a company officer or property owner, so as to preclude the shifting of liability onto AI (Ohio Capital Journal, n.d.); similar initiatives have been introduced in other states, notably Oklahoma. On 8 October 2026 India announced the forthcoming publication of a consultation paper on AI regulation focused on safety, cybersecurity and protection against harmful applications, deepfakes in particular — yet another major jurisdiction moving from soft rules towards framework regulation. Taken together, these developments confirm two propositions that are important for this article: a person's digital likeness is becoming an autonomous object of legal protection, and human-like AI systems are becoming the subject of a special regime defined by their function; at the same time, liability remains with the person or organisation acting through AI.

For Ukraine, open questions remain as to whether a separate right to one's digital likeness is needed and where its boundary with the freedom of satire and parody should lie, as well as how to protect vulnerable groups and allocate the liability of providers. These questions should be resolved in the national model law on artificial intelligence at once, rather than postponed or settled by the mechanical borrowing of foreign solutions; the model of the AI digital human proposed below provides an institutional basis for doing so.

## II. RELEVANCE, AIM AND METHODOLOGY OF THE STUDY

The relevance of the study stems from the fact that legislators in various jurisdictions are already shaping special regimes for a person's digital likeness and for human-like AI systems, whereas doctrine has offered neither operational criteria for distinguishing between digital formations nor mechanisms that would prevent the status of AI from being used as a "liability shield". The scientific novelty of the article lies in the fact that, for the first time, the diagnostic model of "punctuated equilibrium" is combined with constructive models of the legal status of AI subjects; the principle of non-mimeticity is formulated as the theoretical foundation of legal personhood in virtual environments; and a two-branch system of AI legal subjects is proposed, with an original catalogue of rights, four absolute limits, a reserve ratio and a six-tier liability cascade.

The aim of the article is to combine three levels of analysis:

1) the explanatory model of the development of the debate proposed by the foreign colleagues C. Novelli, L. Floridi, G. Sartor and G. Teubner (Novelli et al., 2024);

2) the concept of the AI digital human previously developed by the authors (Onyshchenko and Kostenko, 2026);

3) the system of AI legal subjects of the Metaverse built on the principle of non-mimeticity, which is set out for the first time in this article.

The methodological basis comprises the formal-dogmatic and comparative-legal methods, a functional comparative analysis of competing constructs, the method of legal modelling and the operationalisation of technical features of autonomy on the basis of the ISO/IEC 42001, IEEE 7001-2021 and NIST AI RMF standards (ISO/IEC, 2023; IEEE, 2021; NIST, 2023).

## III. THE "PUNCTUATED EQUILIBRIUM" MODEL OF THE DEBATE ON AI LEGAL PERSONHOOD: THE STUDY BY C. NOVELLI, L. FLORIDI, G. SARTOR AND G. TEUBNER

The central hypothesis of the foreign colleagues is that the scholarly and policy debate on the legal personhood of AI develops according to a model of "punctuated equilibrium" borrowed from evolutionary biology and public policy theory: long periods of relative stability (stasis) are interrupted by rapid paradigm shifts (punctuations) triggered by technological breakthroughs and socio-legal catalysts (Novelli et al., 2024). In routine periods, issues are processed incrementally by specialist subsystems (committees, agencies, professional networks); a punctuation occurs when the problem is reframed and moves to the level of macro-political institutions, where institutional friction is lower and large-scale change becomes possible.

The researchers identify five factors: the first three structure the shifts, while the last two modulate the depth and durability of each equilibrium:

1) the competition between conceptions of legal personhood — singularist and cluster;

2) the state of AI technology, its accessibility and commercial reach;

3) AI's participation in socio-digital institutions;

4) the interaction and internal consistency of adjacent legal regimes (data protection, agency, liability, cybersecurity);

5) the existence or scarcity of judicial precedents on extending legal personhood to new entities (Novelli et al., 2024).

*A. Singularist and cluster conceptions of legal personhood*

The singularist conception proceeds from a minimal understanding: an entity is a person in law if it holds (or is capable of holding) at least one right or duty. This logic is used to justify the protection of animals, foetuses, trees or rivers as bearers of a "legally protected interest" (Stone, 1972). The cluster conception, developed most fully by V. Kurki (Kurki, 2019), treats legal personhood as the vesting of a large "bundle" of legal roles — the capacity to contract and own property, protection against harmful conduct, procedural powers and liability for one's own wrongful conduct; this bundle may be restricted, as is the case for minors or for legal persons, which cannot be spouses or bearers of political rights (Novelli et al., 2022).

Of fundamental importance for the further analysis is the foreign colleagues' conclusion that the choice of conception not only describes the tempo of the debate but also influences it. Singularist logic tends towards stasis: the decision is binary (a single right either exists or it does not), and each new technological capability is "absorbed" in isolation, without systemic reconfiguration. Cluster logic requires the systemic selection of legal positions and their correlates and therefore opens space for normative discretion, broader debates and punctuations. The pragmatic advantage of the cluster model is that it does not depend on identifying a single "foundational" attribute — rationality, consciousness or dignity — and treats legal personhood as a modular package of legal positions that the legislator combines according to functional goals (Novelli et al., 2024). The comparison of the conceptions is summarised in Table 1.

TABLE 1.
**Singularist and cluster conceptions of legal personhood as applied to AI**

| Criterion | Singularist conception | Cluster conception |
|---|---|---|
| Threshold of recognition | a single right or duty | a bundle of legal roles, possibly with restrictions |
| Typical examples in law | animals, rivers, natural objects as bearers of a protected interest | human beings, legal persons; minors and incapacitated persons — with restrictions |
| Typical question about AI (1980s–1990s) | "Can a program be an author?", "Can a robot owe a duty in tort?" | "What set of rights and duties can be granted to an agent that concludes contracts?" |
| Effect on the dynamics of the debate | tendency towards stasis; incremental absorption of technologies | room for discretion; broader debates and punctuations |
| Social personhood (after N. Luhmann and G. Teubner) | not recognised: the entity is merely protected; communication from it has no legal effect | recognised: the entity is an addressee of duties and capable of legally significant communication |

*Source: compiled by the corresponding author based on (Novelli et al., 2024; Kurki, 2019).*

The foreign colleagues link the distinction between the conceptions to a sociological approach to the person: to be a person means to be a partner in communication, that is, someone capable of autonomously producing meaningful utterances and interpreting those of others (Teubner, 2018). The law recognises the social personhood of an entity when it confers on it a cluster that includes powers and duties; the mere legal protection of an entity (a forest, a mountain, an animal) does not amount to such recognition.

*B. Technology as a factor: periodisation of the debate*

On the basis of a systematic literature review, the researchers reconstruct four punctuations (Fig. 1). The first cracks in doctrinal stasis appeared in the late 1960s and early 1970s, when symbolic expert systems (Dendral, Mycin) left the laboratory; in parallel, Roe v. Wade (1973) and C. Stone's essay on the legal standing of trees (Stone, 1972) unsettled traditional notions of the person. Between 1978 and 1985 the first legal works appeared (D. Tuchler, T. Butler, M. Gemignani, M. Willick), examining individual rights — authorship and tort liability — and advancing the idea of "partial personhood". In the early 1990s L. Solum's essay appeared, in which the question of AI as a trustee and as a bearer of constitutional rights served as a pragmatic test of the very concept of legal personhood (Solum, 1992).

The third punctuation is associated with the spread of statistical AI and machine learning in the late 2000s: the debate shifted towards agents capable of autonomous interaction, concluding contracts, paying taxes and even committing crimes (Chopra and White, 2011). The fourth punctuation falls in 2017 — the European Parliament's Resolution on Civil Law Rules on Robotics (European Parliament, 2017) and the "citizenship" of the robot Sophia; afterwards the number of publications on AI legal personhood rose sharply, and citations of Solum's essay doubled. This period is characterised by interdisciplinarity, empirical studies and a certain pessimism about granting AI broad legal personhood (Floridi and Taddeo, 2018; Bryson et al., 2017). Among the works the foreign colleagues cite as evidence of the interdisciplinary turn is a study by Ukrainian and European experts on the methodological problems of reasoning about the "legal personality" of AI (Kostenko et al., 2024a).

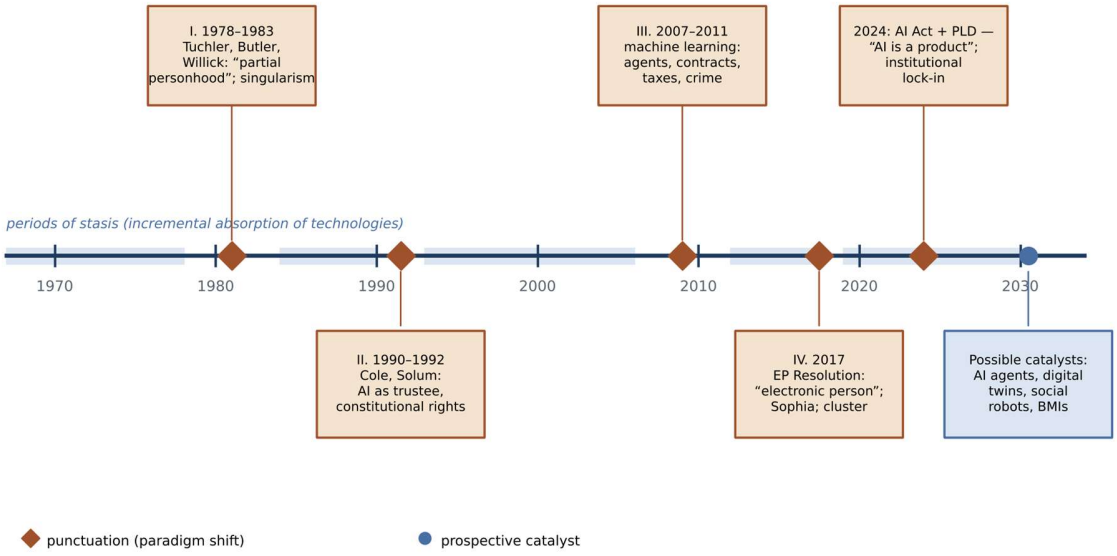



Fig. 1. Punctuations and periods of stasis in the debate on AI legal personhood

*Source: compiled by the corresponding author based on the reconstruction in (Novelli et al., 2024); prospective catalysts follow Section 7 of that work.*

### *C. AI's participation in socio-digital institutions*

The third factor — AI's participation in socio-digital institutions — operates as a feedback mechanism: it sustains stasis when the expectations it generates align with existing law and amplifies punctuation when social personification outpaces legal doctrine. When social communication "institutes" non-human entities as quasi-actors, an almost irresistible institutional pressure is exerted on the law to recognise their (limited or full) legal personhood (Novelli et al., 2024; Beckers and Teubner, 2022). Autonomous algorithms are already institutionalised as market actors in principal–agent relations, and economists observe the agency problems of disloyalty typical of such relations.

The most constructive part of the foreign colleagues' study is the distinction between three types of socio-digital institution, each with its own risks and corresponding liability regimes (Table 2), which draws on the concept of "three liability regimes" developed by A. Beckers and G. Teubner (Beckers and Teubner, 2022).

TABLE 2.
**Types of socio-digital institution and the proposed liability regimes**

| Type of institution | Content and risk | Proposed legal regime |
|---|---|---|
| Digital assistance | the delegation of a task from a human to an algorithm creates a principal–agent relation; causal risks are transformed into action risks (disappointment of expectations about the agent's conduct) | limited legal personhood of the software agent in the principal's interest; the agent's decisions bind the principal; vicarious liability of the user/operator; strict product liability rules are considered inadequate |
| Digital hybridity | dense human–algorithm interaction gives rise to a collective actor; the contribution of each cannot be isolated | enterprise liability in two steps: attribution of the act to the hybrid as a collective, then allocation of liability among the network nodes; primary liability of the hub enterprise with a right of recourse |
| Digital interconnectivity | "collectivity without a collective" — the distributed cognition of a crowd of interconnected algorithms only loosely coupled with human communication | sectoral liability funds with contributions proportionate to market share and problem-solving capacity; orientation towards compensation, prevention and recovery |

*Source: compiled by the corresponding author based on (Novelli et al., 2024; Beckers and Teubner, 2022).*

### *D. Legislative attempts and judicial uncertainty*

As the researchers show, the practical implementation of theoretical proposals has been minimal, and the main obstacle lies in cross-domain regulatory linkages, above all with liability regimes. The only formal conferral of "personhood" on AI was the citizenship granted to the robot Sophia in Saudi Arabia (2017), which had no legal consequences whatsoever and is regarded as "political choreography" in favour of the social robotics market. The European Parliament's proposal on "electronic personhood" (para. 59(f) of the Resolution) (European Parliament, 2017) met with resistance, including an open letter signed by 156 experts from 14 countries. The critics' central argument is the risk of a "liability shield": separate legal personhood for AI could allow manufacturers and developers to shift liability onto an artificial person without assets (Bryson et al., 2017; Chesterman, 2020). Moreover, unlike a corporation, an AI system lacks an identifiable circle of stakeholders, a stable asset pool and an intelligible organisational purpose, and it is not even clear

which layer of the technology (the model, the training data, the deployed instance or a socio-technical ensemble) would constitute the "person" (Novelli et al., 2024).

This scepticism was shared by the European Commission's Expert Group on Liability and New Technologies, which advocates strict liability for high-risk AI, control-based liability, compulsory insurance and an easing of the burden of proof (Expert Group on Liability and New Technologies, 2019). In the researchers' view, the EU regulatory triad has definitively entrenched the principle that "AI is a product, not a subject with autonomous status", so the debate in the EU will remain largely inactive in the coming years (Novelli et al., 2024).

Case law presents a mixed picture. According to N. Banteka, in US court decisions the main condition for recognising a person is the existence of a statutory basis (45% of cases), the second is the "right to sue and be sued" (15%), and the third is whether the entity is an aggregate of individuals (Banteka, 2021). The foreign colleagues draw attention to the circularity of this reasoning: courts treat as prerequisites of legal personhood what are in fact its consequences. At the same time, the case law of other legal orders is more activist: German courts have recognised the legal personhood of partnerships and trade unions without an express statutory basis, courts in the Global South have personified rivers, and the Beijing Internet Court in Li v. Liu (2023) granted protection to an AI-generated image while attributing authorship to the human who formulated the prompts. The researchers conclude that the recognition of AI as a full person will first require it to acquire de facto legitimacy — the sustained performance of roles involving the exercise of rights and duties within socio-digital institutions, similar to the historical path of corporations (Novelli et al., 2024).

### *E. The foreign colleagues' forecasts and proposals*

In the near to medium term, the researchers forecast no radical shift: liability and intellectual property rules create a "lock-in" effect — firms build their risk management around them, and insurers price cover on the assumption that the defendant remains human. Instead, taxonomically differentiated regulation of AI itself is expected along the lines of the AI Act — distinguishing specialised from foundation models and levels of risk and forming a "spectrum of personhood" where it adds clear value (Novelli et al., 2024).

The potential catalysts of future punctuations identified are: the growing creativity of generative AI, which shapes public perceptions of its autonomy; the recognition of algorithms as autonomous contracting parties (with a shift from strict product liability to vicarious liability) (Kolt, 2025); the emergence of AI agents autonomously conducting long-term economic activity; personalised avatars and digital twins functioning as extensions of their users (Cheong, 2024); social robots; and, in the long term, the integration of AI with brain–machine interfaces (BMIs). The latter may reframe the question from "AI as a separate subject" to "AI as an extension of the natural person" or, in the logic of actor–network theory, to the legal personhood of hybrid human–machine associations. At the same time, in the researchers' assessment, social robots and digital twins are unlikely on their own to break the current equilibrium, since they do not change the cognitive capabilities of machines (Novelli et al., 2024).

### *F. Assessment: what the model explains and what it does not offer*

The foreign colleagues' model is highly adequate: it explains why the debate is cyclical, why the cluster approach stimulates punctuations and why legislative initiatives fade within the dense network of adjacent EU regimes. It also accurately identifies two practical obstacles — the risk of a "liability shield" and the circularity of judicial criteria — and draws an important conclusion about the role of de facto legitimacy. Nevertheless, the model is predominantly diagnostic. First, it offers no operational criterion for distinguishing between digital formations; in particular, it does not differentiate the digital reflection of a specific person from an autonomous formation without a prototype, even though digital twins and personalised agents are named among the likely catalysts. Second, it identifies the risk of a "shield" but proposes no institutional mechanism that would turn status into a source of security rather than evasion. Third, its scale of legal personhood, as in gradient models (Mocanu, 2022; Novelli, 2023), remains tied to the degree of approximation to a human being or a corporation. It is precisely these gaps that the two authorial models set out below are intended to fill.

## IV. THE AI DIGITAL HUMAN AS A NEW CLASS OF DIGITAL LAW SUBJECT

### *A. Starting points: the three-class model and the criterion of connection to a prototype*

Earlier research proposed a three-class model of AI legal subjects based on the criterion of the degree of autonomy and the functional role of the system, with a rebuttable presumption of class (Kostenko, 2025). Class 1 covers instrumental AI systems without independent procedural or proprietary legal personhood (liability rests with the operator, developer or user under the general rules of tort). Class 2 covers systems with limited functional legal personhood acting within a clearly defined registered "electronic mandate", by analogy with agency. Class 3 covers systems with a high degree of autonomy, for which a "chain of liability" is advocated between the developer, the operator and — where the relevant registration status exists — the system itself within a segregated asset fund. The model was developed in debate with N. Banteka's thesis of an "inverse spectrum" of liability, according to which the liability of the human operator should increase as autonomy grows (Banteka, 2021); the rational core of this thesis is accommodated through the subsidiary liability of the operator for Class 3.

In the technical and marketing literature the term "digital human" covers everything from photorealistic avatars to conversational agents based on large language models. The legal meaning of the term is determined by the answer to a single question: is there a stable, legally significant connection between the digital formation and a specific, identified natural person (Onyshchenko and Kostenko, 2026)? This parameter — the presence or absence of a connection to a prototype — remains undeveloped in the Western literature, in particular in gradient models, which build the scale of legal personhood

exclusively around the functional features of the system itself (Mocanu, 2022).

The answer to this question divides "digital humans" into two modules. Module 1 (AI-DH-NP; Digiperson) is the functional reflection of a natural person whose attributes are derived from those of a real human being and serve that person's access, identification, exercise of rights and performance of obligations in the digital world. Module 2 (autonomous AI-DH; autonomous Digihuman) is a formation that reflects no real person, its attributes being formed referentially for a specific function within a digital ecosystem. Every Digiperson is a variety of Digihuman, but not every Digihuman is a Digiperson. For Module 1 the central problem is authentication and protection against substitution (the legal analogue of identity theft); for Module 2 it is deceptive anthropomorphisation.

*B. Module 1 (Digiperson): the digital reflection of a natural person*

A Digiperson should be built primarily on the "red-group" identification attributes — attributes of heightened sensitivity whose alteration or compromise entails the most significant legal consequences (biometric data, the particulars of identity documents, qualified electronic signatures) (Kostenko, 2021) — together with derived access attributes: an electronic identifier, qualified electronic attestations of attributes in the terminology of eIDAS 2.0 (Regulation (EU) 2024/1183, 2024) and access tokens. It is fundamental that these attributes are not created arbitrarily but are digitised or derived from an existing body of a real person's data under an established verification procedure; constructing "plausible" but unverified attributes under the guise of a real prototype takes the formation outside Module 1 and should be classified as digital fraud.

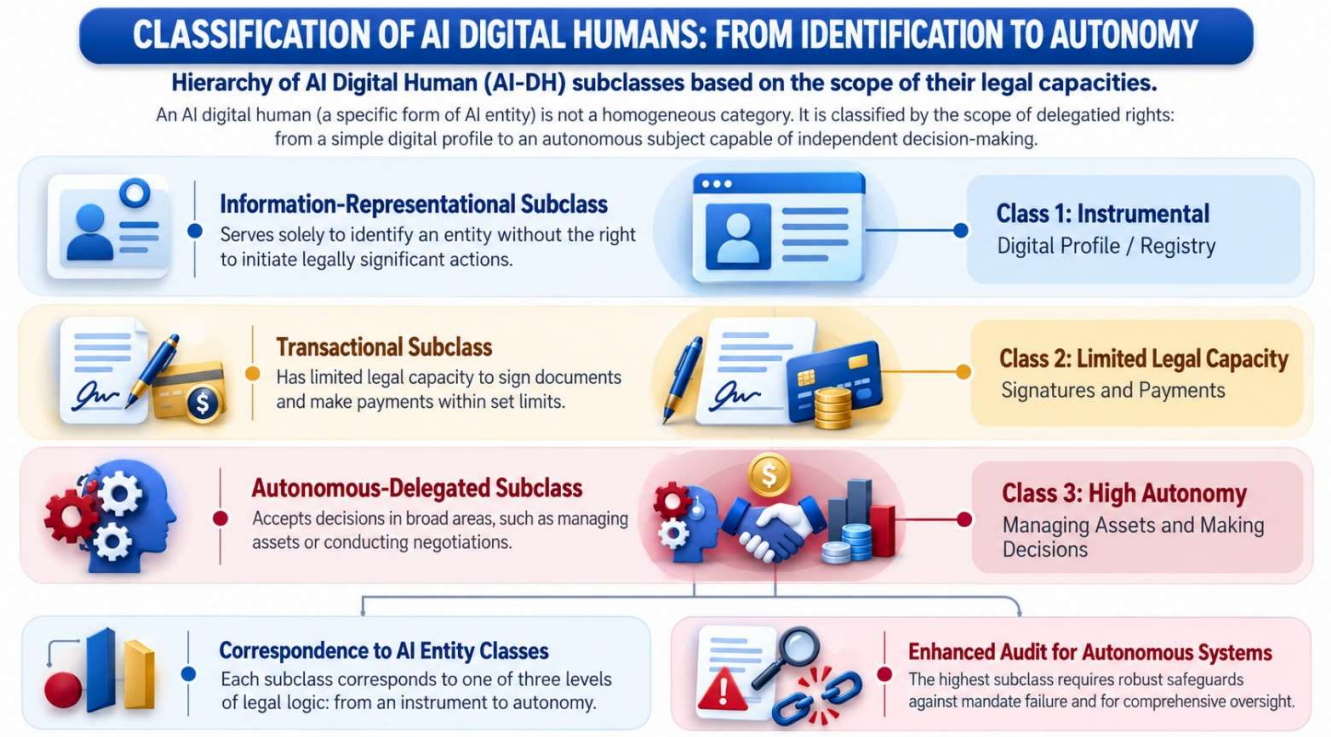



Fig. 2. Hierarchy of subclasses of the AI digital human reflecting a natural person (Digiperson)

*Source: compiled by the corresponding author based on (Onyshchenko and Kostenko, 2026).*

According to the scope of delegated authority, three subclasses of Digiperson are distinguished (Fig. 2): the information-representational subclass (presentation of attributes for identification only, without the right to perform legally significant acts), the transactional subclass (a limited mandate to sign documents and make payments within set limits) and the autonomously delegated subclass (an extended mandate to manage digital assets or conduct negotiations, with enhanced audit and the possibility of immediate revocation). The subclasses correspond directly to Classes 1–3 of the three-class model.

The central doctrinal caveat is the principle of incomplete identity: the digital reflection does not automatically inherit the full scope of the rights and obligations of the prototype natural person. It is proposed to build the scope of a Digiperson's active legal capacity by analogy with the age-based gradation found in civil law — a "digital child" (information-representational properties only), a "digital adolescent" (a limited range of operations, analogous to the partial capacity of minors) and an "adult digital human" (an extended mandate that approaches, but does not equal, the full capacity of the prototype and always remains derivative and revocable). The analogy concerns only the technique of differentiating the scope of capacity and does not extend to the digital reflection the status of a human being as a bearer of dignity. The principle has practical consequences on three planes: harm caused within the mandate is attributed to the prototype or to an operator authorised by them under the rules

on a principal's liability; a Digiperson cannot be a party to court proceedings in its own name; and the rights to honour, dignity, business reputation and privacy remain the rights of the prototype (Onyshchenko and Kostenko, 2026).

A Digiperson should be distinguished from related concepts. An engineering "digital twin" is an instrument for modelling a physical object, not for representation; an "electronic avatar" is a means of visually representing the user, controlled by them in real time. A Digiperson occupies an intermediate position: unlike an avatar, it acts within its mandate without synchronous human control; unlike a twin, it exercises the prototype's rights and obligations rather than modelling their physical state.

*C. Module 2: the autonomous Digihuman*

An autonomous AI digital human is created without borrowing the attributes of a real person: its name, visual image, communicative style and declared competence are constructed by the operator for its functional purpose. This module includes autonomous customer assistants of financial and insurance platforms, non-player characters (NPCs) in Metaverse and educational environments, and advisory agents of e-government portals. Mechanisms of protection against "digital identity theft" do not apply to Module 2 — there is no person whose identity could be stolen; instead, an obligation to disclose the artificial nature of the interaction applies, akin to Article 50 of the AI Act (Regulation (EU) 2024/1689, 2024). The intensity of disclosure is differentiated: continuous labelling in every session for financial assistants, a one-off notice for educational and entertainment NPCs, and disclosure combined with a mandatory indication of how to switch to a human official for e-government agents. A comparison of the modules is given in Table 3.

TABLE 3.
**Comparative characteristics of the modules of the AI digital human**

| Criterion | Module 1 (Digiperson) | Module 2 (autonomous Digihuman) |
|---|---|---|
| Connection with a real prototype | present and verified | absent by definition |
| Source of attributes | digitised / derived attributes of the prototype ("red group" and derivatives) | referentially formed attributes tied to function |
| Principal legal risk | identity substitution, compromise of the mandate | deceptive anthropomorphisation |
| Key obligation of the operator | verification of the connection with the prototype, protection of the mandate | disclosure of the artificial nature of the interaction (Art. 50 AI Act) |
| Correspondence with the three-class model | Classes 1–3 depending on the subclass | mostly Class 1, occasionally Class 2 |
| Registration regime | superstructure over the national e-identification system (analogous to the EUDI Wallet) | independent sectoral register by analogy with the register of legal persons |

*Source: compiled by the corresponding author based on (Onyshchenko and Kostenko, 2026).*

*D. The Digital Humans Registry and the comparative-legal dimension*

A Digital Humans Registry is proposed as a common instrument of legitimation for both modules. For Module 1 it records the verified connection with the prototype, the subclass and the term of the mandate; for Module 2 — the operator, the functional purpose, a declaration of the absence of any connection with a real prototype and the person responsible. Registration is declaratory as regards the emergence of functional status but constitutive for the purposes of the presumption that third parties are aware of the scope of the digital human's authority. For Module 1 the registry should be designed as a superstructure over the electronic identification infrastructure, compatible with the logic of "user-controlled attributes" of the European Digital Identity Wallet (Regulation (EU) 2024/1183, 2024).

Comparative analysis shows that the gap is global rather than national. The AI Act builds regulation on risk assessment irrespective of whether the system is connected to a specific person; this suffices for product safety but not for private law: a transactional Digiperson and an autonomous advisory agent of the same risk level require fundamentally different regimes of liability, counterparty identification and data protection (Regulation (EU) 2024/1689, 2024). The Framework Act of the Republic of Korea on the Development of Artificial Intelligence and Establishment of Trust (adopted on 26 December 2024, in force since 22 January 2026) declares the protection of human dignity as a regulatory goal but likewise contains no category of "digital human" (Republic of Korea, 2025). The closest existing analogue of the proposed right to non-algorithmic existence is Article 22 GDPR (Regulation (EU) 2016/679, 2016), which, however, concerns decisions by third parties and does not cover decisions taken in a person's name by that person's own digital reflection.

*E. Digital dignity: the non-simulacrum principle and the right to non-algorithmic existence*

The institution of the AI digital human is developed within the framework of the doctrine of digital dignity, which the authors elaborate within the concept of Grand Lex Digitalis (Kostenko and Zhuravlov, 2025). The non-simulacrum principle means that no digital formation may mislead the user as to its nature: a Digiperson does not conceal that the expression of will is made not by the prototype but by its reflection within the mandate; an autonomous Digihuman does not present itself as a real person. The principle develops J. Bryson's warning about the harm of anthropomorphising autonomous systems (Bryson, 2010). The right to non-algorithmic existence is the right of a natural person to require that statutorily defined categories of decisions (concerning restrictions of rights, health, parental relations or significant sums) be taken by them personally rather than by the autonomously delegated subclass of Digiperson, even where

the mandate formally permits this. This right cannot be waived in advance and in general terms.

A Digiperson of the transactional and autonomously delegated subclasses is a particular case of the broader institution of the AI representative, which has three levels: the AI representative of a public authority (a public-law mandate with the highest level of transparency), the AI representative of a legal person (a mandate based on an internal act, registered by analogy with a power of attorney) and the Digiperson as the representative of a natural person (a mandate based on individual will, with a right of immediate and unconditional revocation). This makes it possible to propose a single chapter of the draft law on delegated digital legal personhood instead of separate sections on "digital humans" and "AI representatives" (Onyshchenko and Kostenko, 2026). The institution of the AI representative is developed into a full typology in Section V.

## V. A SYSTEM OF AI LEGAL SUBJECTS OF THE METAVERSE BASED ON THE PRINCIPLE OF NON-MIMETICITY

### *A. The mimetic trap and the principle of non-mimeticity*

Existing legal constructs — the avatar, the digital twin, "digital humans", electronic personhood and the AI avatar as a quasi-subject (Cheong, 2024) — share a common feature that has not so far been problematised: they are mimetic, that is, they construct the new subject as a reflection of the human being. The consequences of this choice are fundamental rather than technical. The first is the dispute over consciousness and intent: if a subject is defined as a likeness of a human being, the question of whether it possesses consciousness becomes legally relevant, although the law has no means of answering it (Solum, 1992; Chesterman, 2020). The second is the problem of dignity: an affirmative answer devalues the uniqueness of the human person, while a negative one destroys the mimetic premise itself. The third is the risk of substituting the subject, on which the strongest criticism is built (Bryson et al., 2017; Banteka, 2021). The fourth is the unverifiability of criteria: likeness to a human being has no measurable indicator and cannot be the object of certification.

The principle of non-mimeticity defines a subject differently — through its registered function and verified level of autonomy; the feature of likeness to a human being is removed from the legal composition altogether. The question of consciousness is not resolved but set aside: it does not form part of the conditions for acquiring status. This construction is not new to law as such. The legal person — the most successful non-natural subject in legal history — was never a copy of a human being: it has no body, consciousness or intent in the psychological sense, and it is for precisely this reason that theory moved early from the search for its "will" to a description of its organisational and proprietary structure and the mechanism for attributing acts to it. The classical doctrine of the legal person, the cluster theory (Kurki, 2019) and conceptual frameworks for the divisibility of legal personhood (Novelli et al., 2022) are in this sense non-mimetic by construction. Hence an AI legal subject is not a digital duplicate of a human being but a new type of non-natural subject placed in the same series as the legal person. The principle gives concrete subject-related content to the non-simulacrum principle formulated within the architecture of a digital code (Kostenko and Zhuravlov, 2025).

### *B. The two-branch taxonomy of the system of AI subjects*

The system of AI legal subjects is the totality of statutorily provided types of autonomous software and organisational entities endowed with the capacity to perform legally significant acts in virtual and informational environments within a registered profile, subject to a verified level of autonomy, deposited proprietary security and the technical reversibility of their acts. The system has two branches (Fig. 3). The status branch is delimited by autonomy class; its single type is the AI legal entity, which acts in its own name within a registered profile and holds a segregated digital estate. The representative branch is delimited by the principal and the delegated function; its types are AI representatives, which act on behalf of a defined principal within a digital mandate, with attribution of will to that principal.

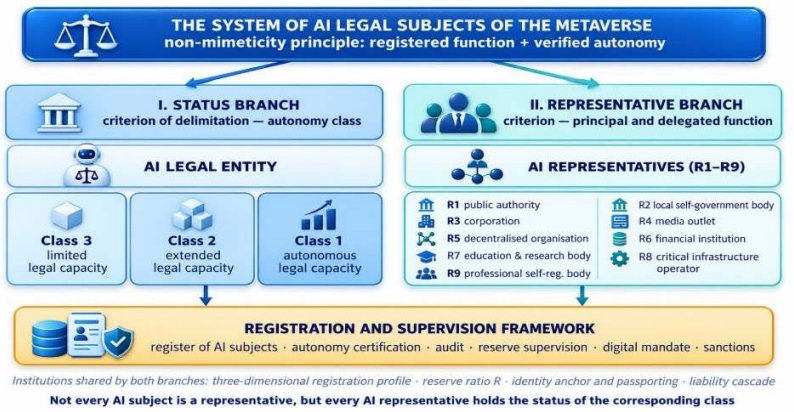



Fig. 3. Architecture of the system of AI legal subjects of the Metaverse

*Source: compiled by the corresponding author.*

The relationship between the branches may be stated as follows: not every AI subject is a representative, but every AI representative must hold the status of the corresponding class. Representation is a function, not a status; it is superimposed

on a classified subject and does not replace it. A single-branch system would be incomplete in either form: the status branch would not cover action on behalf of a public authority, an editorial office or a corporation, while the representative branch would not cover autonomous entities without a principal, in particular memberless organisations (Bayern, 2021; Bayern et al., 2017).

### *C. The status branch: the AI legal entity and autonomy classes*

The autonomy class is established through a certification procedure on the basis of five legally significant criteria, each derived from a technical property of agency and supported by a verification instrument based on existing standards (ISO/IEC, 2023; IEEE, 2021; NIST, 2023) (Table 4). For the status branch, a rank numbering of classes is used in which a lower number denotes broader legal capacity: Class 3 — limited, Class 2 — extended, Class 1 — autonomous legal capacity (the correspondence with the scale in Section IV is shown in Table 6). The legal form of all the criteria is a rebuttable presumption of class: a system certified against a defined profile is presumed to belong to the corresponding class until the presumption is rebutted by the findings of an extraordinary audit. This mechanism relieves the court of ad hoc technical expertise in every case and transfers the question of fact to the sphere of certification — just as the law of technical regulation does with regard to product safety.

TABLE 4.
**Features of autonomy and classes of the AI legal entity**

| Legal criterion | Verification instrument | Class 3 — limited | Class 2 — extended | Class 1 — autonomous |
|---|---|---|---|---|
| Closure of the decision loop | decision logging under ISO/IEC 42001; NIST AI RMF | decisions only within the operator's instructions | independent decisions within a defined field | independent goal-setting within the registered purpose |
| Capacity to conclude transactions independently | certification testing of expressions of will; transaction protocols | does not transact in its own name | transactions from an approved list | transactions without a list, subject to statutory exclusions |
| Severability of digital assets | asset accounting; distributed register of property | assets not attached | limited segregated estate | full estate with a public register of changes |
| Auditability of behaviour | IEEE 7001-2021; event logs; post-deployment monitoring | basic logging | mandatory annual audit | continuous monitoring and extraordinary audits |
| Controllability (Art. 14 AI Act) | conformity assessment; ISO/IEC 23894 | continuous operational control | supervisory control with a right of intervention | ex post control; mandatory immediate suspension mechanism |

*Source: developed by the corresponding author based on (ISO/IEC, 2023; IEEE, 2021; NIST, 2023; Regulation (EU) 2024/1689, 2024).*

What is at issue is operational rather than cognitive autonomy: the law does not assess whether a system possesses consciousness, only its ability to perform legally significant functions in a stable and predictable manner without continuous human intervention. This is also a response to gradient models (Mocanu, 2022; Novelli et al., 2022): the divisibility of status is accepted, but the scale is built on verified autonomy rather than on the degree of approximation to a human being. The liability regime is differentiated: for Class 3, harm is compensated by the operator irrespective of its cause; for Class 2, the primary source of satisfaction is the subject's segregated estate, with the operator liable on a subsidiary basis; for Class 1, the subject's own proprietary liability is primary, and the operator is liable only in cases defined by statute (covert intervention, circumvention of audit, manipulation of algorithms or use of the system for unlawful activity). Class 1 is an exceptional status, and it is precisely the restriction of its scope that secures the proportionality of regulation.

### *D. The catalogue of rights of an AI subject and the four absolute limits*

If an AI subject is not a duplicate of a human being, its rights cannot be formed by "trimming" the catalogue of human rights (removing electoral, family and personal non-property rights and retaining "the remainder") — such a method is mimetic by construction. The catalogue is built from functional necessity: a right is included if and only if, without it, the subject cannot perform its registered function or defend its own status in the procedures provided by law.

Four tiers of rights result.

Registration rights (arising upon entry in the register): the right to a digital identifier and its immutability, to the integrity of the registered model and to access to register data concerning itself.

Property rights (from Class 2): the right to hold a segregated digital estate, to manage it and to conclude transactions within a defined field — not a benefit for the subject but a condition for securing the claims of injured parties.

Procedural rights: the right to an audit procedure before a class downgrade, to appeal against the suspension of status and to procedural representation in disputes concerning its own status; formally they belong to the subject, functionally they serve legal certainty in commerce.

Representative rights (in the representative branch only): the right to act on behalf of the principal within the digital mandate and to require from the principal the information needed to perform the delegated function.

The catalogue is closed by four absolute limits that depend neither on the autonomy class, nor on the type of representation, nor on the technical level of the system:

1) human rights and rights derived from them, including electoral, family and personal non-property rights, as well as dignity — their basis is human nature;

2) public-authority discretion and the final determination of matters restricting constitutional rights — democratic legitimacy is a property of a human decision;

3) the recursive creation of legal subjects — the chain of legal personhood must remain anchored to a human decision;

4) the independent alteration of one's own class, profile or register entry — the principle of no self-evolution and of State control over the composition of legal subjects.

None of the limits results from the technical imperfection of systems, and accordingly no technical improvement weakens them. Mimetic constructs cannot in principle possess this quality: within them a limit always appears provisional, because it is defined by the degree of approximation to a human being.

*E. The representative branch: nine types of AI representative*

The classical model of representation in every branch of law rests on the premise that legally significant acts on behalf of another person are performed by a human being whose will is the source of the powers and the guarantee of their proper exercise. The legal nature of an AI representative differs in four respects: the source of the powers is not a power of attorney or an employment contract but a statute, an administrative act or a decision of the principal's organ combined with registration; the scope of the powers is determined not by personal discretion but by a software-and-normative profile; every act is subject to automatic logging and audit; and the powers may be suspended instantly by the regulator. The common mechanism is the digital mandate — not a document but a set of legally defined parameters recorded simultaneously in the register and in the system's software profile (the boundaries of competence, the permitted types of act, temporal and territorial restrictions, quantitative limits, rules on automatic suspension and logging conditions). Acts outside the mandate produce no attribution of will to the principal. The typology is set out in Table 5.

TABLE 5.
**Types of AI representative: principal, delegated scope and negative list**

| Type | Principal | Delegated scope | Negative list (never delegated) |
|---|---|---|---|
| R1 | public authority | processing of applications, preparation of draft decisions, automated administrative services within non-discretionary competence | final decisions restricting constitutional rights; discretionary acts; sanctions |
| R2 | local self-government body | municipal e-services, residents' applications, administration of local registers | disposal of communal property; town-planning discretion |
| R3 | corporation | electronic contracts, compliance, financial monitoring, corporate record-keeping | decisions of the general meeting; approval of major transactions |
| R4 | media outlet (editorial office) | selection, aggregation, preparation and dissemination of content labelled as machine-generated | editorial policy; publication of material concerning private individuals without human approval |
| R5 | decentralised organisation | execution of protocol decisions, representation before registers, asset management | amendment of the protocol; issuance outside a members' decision |
| R6 | financial institution | scoring, underwriting, execution of client instructions, reporting | final refusal of access to a financial service without review |
| R7 | education and research institution | administration of the educational process, academic integrity checks, research infrastructure | final assessment; findings of academic plagiarism |
| R8 | operator of critical infrastructure | monitoring, dispatching, incident response under the regulations | decisions to disconnect critical facilities; emergency regimes |
| R9 | professional self-regulatory body | maintenance of registers, administration of admission, disciplinary record-keeping | disciplinary decisions on the merits; admission to the profession |

*Source: developed by the corresponding author. The criterion of permissible delegation is the principle of functional admissibility: only powers that rest on clear normative criteria, do not call for broad discretion, can be fully logged and remain subject to subsequent human review may be delegated.*

The most sensitive type is R1, since it comes into contact with a person's right not to be subject to a decision based solely on automated processing (Regulation (EU) 2016/679, 2016). The construct resolves this conflict not by an exception to the right but through the scope of delegation: R1's competence covers only acts culminating in a draft decision, or decisions within non-discretionary competence with a mandatory opportunity for human review; the negative list should be enacted expressly in statute. Type R4 is where the difference between a duplicate of a human being and an autonomous subject emerges most sharply: a generative system is not a "digital journalist", does not acquire journalistic rights derived from the human freedom of expression, is not an author and has no editorial independence; liability for the information disseminated rests with the editorial office as principal.

*F. Portability and reversibility of status*

An autonomous subject is multi-world by nature, whereas a corporate "wrapper" ties it to a single jurisdiction and platform rules tie it to a single world. The identity anchor is a unique, cryptographically verifiable identifier that links the AI subject to its register entry and carries a minimum set of machine-verifiable particulars: the type and branch of the subject, its autonomy class, functional profile, the parameters of the digital mandate, the date of the last audit, the state of the reserve and any restrictions in force. Its technical basis is the EU digital identity infrastructure (Regulation (EU) 2024/1183, 2024), and its conceptual precursor is the model of a cross-border personalised ID code for avatars and electronic personalities (Kostenko et al., 2024b). Status passporting is a mechanism for the recognition of status by host worlds

modelled on the single licence with notification of the host State in financial law: a subject registered in one legal order acts in another world upon notification of its administrator, without re-registration. The novelty lies in transposing an inter-State institution to the relations between a legal order and a private platform, which is consistent with the conception of digital jurisdiction as a post-territorial legal institution (Kostenko and Zhuravlov, 2025).

An autonomous subject acts faster than human oversight, so an erroneous act may become irreversible before it is detected. Protocol-level suspension is therefore provided for — a technically embedded ability to suspend the subject's activity by decision of the regulator, a court or the operator, with simultaneous freezing of the segregated assets (a condition for certification in Class 1). For the financial stratum (F2–F5), a deferred settlement finality window is introduced: a transaction becomes final not at the moment of execution but upon the expiry of a short regulatory period during which it may be challenged on an exhaustive list of grounds (exceeding the profile or mandate, exceeding a limit, a fall in the reserve below the required level, or technically confirmed compromise). The burden of proof rests on the applicant; the window does not extend to the transactional stratum, where the cost of delay exceeds the benefit of reversibility.

*G. The liability cascade and the life cycle of status*

The liability model has six tiers and is built on the principle of successive exhaustion (Fig. 4); its purpose is to guarantee that in any scenario there exists a person from whose property compensation can be obtained. Tier 0 — attribution of will to the principal — applies only in the representative branch and precedes all the others: where an act has been performed within the digital mandate, its consequences arise directly for the principal, and the question of the AI representative's own property does not arise at all. It is this tier that ensures that an AI representative does not become a buffer absorbing the principal's liability. Tier 3 — the guarantee fund of the platform world — spreads tail risk among the participants of a single environment and gives the world's administrator a direct economic interest in admitting only reputable participants; functionally, it corresponds to the sectoral funds that the foreign colleagues propose for digital interconnectivity (Novelli et al., 2024). Tiers 4 and 5 are consistent with the regime of liability for defective products (Directive (EU) 2024/2853, 2024) but do not apply where the harm was caused by an act within the registered profile in compliance with all standards — otherwise the operator would gain nothing from complying with the rules.

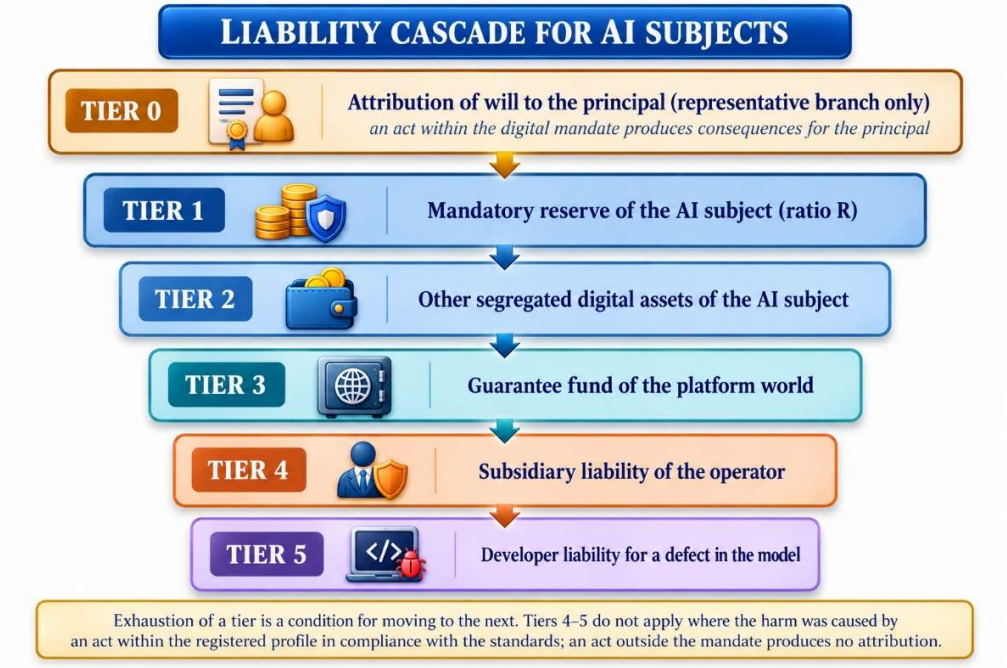



Fig. 4. The six-tier liability cascade with a tier for the attribution of will to the principal

*Source: developed by the corresponding author.*

The status of an AI subject is dynamic: retraining of the model, the addition of new modules and changes in data sources alter the actual autonomy profile. The life cycle comprises six principal stages (the operator's application, autonomy certification, entry in the register, deposit of the reserve, operational activity and periodic audit) and four exit routes (class upgrade, class downgrade, suspension of status and termination with winding-up and distribution of the residual reserve). The construct is closed by two prohibitions. The prohibition of automatic upgrade: deploying a more complex model or increasing the number of parameters does not change status without the official assessment procedure. The prohibition of self-alteration: no AI subject may independently alter its own class or profile, register itself, create another AI subject or confer new powers on itself; such acts are void. This is a direct response to the scenario of recursive self-replication of subjects described as the limit of the applicability of corporate wrappers (Bayern, 2021).

## VI. SYNTHESIS: INSTITUTIONAL RESPONSES TO THE FACTORS OF THE "PUNCTUATED EQUILIBRIUM" MODEL

Comparing the three levels of analysis shows that the authorial models do not compete with the foreign colleagues' explanatory model but complement it with institutional mechanisms precisely where it identifies a problem without proposing a solution (Table 6).

TABLE 6.
**Factors and problems identified by the foreign colleagues and the responses of the authorial models**

| Factor / problem according to (Novelli et al., 2024) | Response of the AI digital human model | Response of the system of AI subjects of the Metaverse |
|---|---|---|
| Competition between the singularist and cluster conceptions | age analogy: graduated expansion of the Digiperson's cluster of roles | the cluster is built from functional necessity (four tiers of rights) with four absolute limits |
| Absence of a foundational attribute of the person (consciousness, dignity) | the criterion of connection to a prototype instead of "human-likeness" | principle of non-mimeticity: consciousness is not part of the legal composition; class is determined by certification |
| Risk of a "liability shield" | liability of the prototype or operator under the rules of agency | reserve ratio R, guarantee fund of the world, cascade with a tier for attribution of will |
| Socio-digital institutions: assistance / hybridity / interconnectivity | three-level AI representative (State — corporation — natural person) | nine types of AI representative with negative lists; the world fund as an analogue of a sectoral fund |
| Circularity of judicial criteria | declaratory-constitutive Digital Humans Registry | rebuttable presumption of class; register, audit and life cycle move the question of fact into certification |
| Catalysts: digital twins, personalised agents | Module 1 (Digiperson) as a separate legal regime | identity anchor and passporting of status between worlds |
| Consistency of adjacent EU regimes | compatibility with the AI Act, eIDAS 2.0 and the GDPR | superimposed regime: the AI Act, eIDAS 2.0 and Directive 2024/2853 are retained in full |
| Scale of classes | Class 1 — instrumental, Class 3 — highly autonomous | rank scale: Class 3 — limited, Class 1 — autonomous legal capacity (instrumental systems remain outside the system of subjects) |

*Source: developed by the corresponding author.*

Two conclusions of the synthesis are particularly important. First, the foreign colleagues regard the acquisition of de facto legitimacy through the sustained performance of roles in socio-digital institutions as a condition for recognising AI as a person. The proposed system does not wait for this to happen spontaneously but creates a controlled environment for its acquisition: the register, certification, audit and passporting make the performance of roles visible, verifiable and reversible, thereby transforming de facto practice into an institutionally formalised status. Second, the researchers forecast that taxonomically differentiated regulation of AI will dominate in the near term. The three-dimensional registration profile (type — class — function) is precisely such a taxonomy, but supplemented by the subject-related dimension that the AI Act lacks. The system of AI subjects does not deny the approach that "AI is a product": the requirements for high-risk systems, human oversight and documentation are retained in full (Regulation (EU) 2024/1689, 2024; Council of Europe, 2024), while status adds a subject-related dimension to them where the classical subject structurally fails — in the case of action without a human decision at the moment of its performance, multi-world presence and memberless organisations.

For the legislation of Ukraine, implementation requires four steps: supplementing the list of participants in civil relations with new types of subjects with special legal capacity (in the Civil Code of Ukraine); aligning the conceptual apparatus with the legislation on virtual assets; enacting the institution of the AI representative in sectoral (administrative, corporate and information) legislation; and establishing the register and the supervisory authority. The proposed articles of the draft Law "On Artificial Intelligence" concerning the AI digital human (the concept, Digiperson, autonomous Digihuman, the Digital Humans Registry, liability and appeal) (Onyshchenko and Kostenko, 2026) should be integrated into a single chapter on delegated digital legal personhood together with the provisions on the AI representative and the AI legal entity.

## VII. LIMITATIONS OF THE STUDY

The proposed models have several limitations. First, the quantitative parameters, above all the reserve ratios, are given as indicative calculations by analogy with prudential regulation; their calibration requires empirical data on the turnover and loss experience of specific platforms. Second, the article does not address the tax consequences of the activity of AI subjects or conflict-of-laws questions concerning the applicable law in a multi-world environment. Third, the effectiveness of status passporting depends on the voluntary accession of world administrators to the register. Fourth, the assessment of the system's effects is prognostic: the Metaverse environment is still taking shape, and there is as yet no practice of applying legislation on the AI digital human in Ukraine. Finally, the analysis of the foreign colleagues' model is based on a working version of their paper published on SSRN, which may be revised (Novelli et al., 2024).

## VIII. CONCLUSIONS

1. The debate on AI legal personhood, as C. Novelli, L. Floridi, G. Sartor and G. Teubner have convincingly shown, develops according to a model of "punctuated equilibrium", and its dynamics are determined by the competition between the singularist and cluster conceptions, the state of technology, AI's participation in socio-digital institutions, the consistency

of adjacent legal regimes and case law. The model has strong explanatory power but is predominantly diagnostic: it identifies the risk of a "liability shield" and the circularity of judicial criteria without proposing institutional mechanisms to overcome them.

2. The concept of the "digital human" requires legal differentiation into Module 1 (Digiperson — the digital reflection of a specific natural person based on verified "red-group" attributes) and Module 2 (an autonomous Digihuman without a prototype). In neither module is the digital human identical to the natural person in the fullness of rights; the scope of a Digiperson's capacity is determined by age analogy and always remains derivative and revocable. The institutional basis for legitimating both modules is the Digital Humans Registry, compatible with the eIDAS 2.0 architecture, while the limits of delegation are set by the non-simulacrum principle and the right to non-algorithmic existence.

3. The principle of non-mimeticity — defining a subject through its registered function and verified level of autonomy rather than through likeness to a human being — does not answer the ontological questions of consciousness and dignity but renders them legally irrelevant. Its historical precedent is the legal person. On this principle a two-branch system of AI legal subjects is built: the status branch (the AI legal entity with three autonomy classes) and the representative branch (nine types of AI representative — from a public authority to a professional self-regulatory body).

4. The rights of an AI subject are formed from functional necessity in four tiers (registration, property, procedural and representative rights) and are bounded by four absolute limits (human rights, public-authority discretion, the recursive creation of subjects and self-alteration of status), which are not weakened by any increase in autonomy.

5. The administrability, security and reversibility of the system are ensured by the three-dimensional registration profile, the reserve ratio with its double progression, the identity anchor with status passporting, the deferred settlement finality window, the six-tier liability cascade with a tier for the attribution of will to the principal and the life cycle of status with the prohibitions of automatic upgrade and self-alteration. The cascade turns status from a potential "shield" into an extension of the proprietary base for compensation.

6. The authorial models provide institutional responses to each of the factors identified by the foreign colleagues and create a controlled environment for AI to acquire the de facto legitimacy that the researchers regard as a precondition for recognition. Prospects for further research relate to the empirical calibration of reserve ratios, the conflict-of-laws regulation of the acts of AI subjects in a multi-world environment, the admissibility of algorithmically processed logs as evidence and the sectoral elaboration of types R1–R9.

## IX. REFERENCES


Banteka, N. (2021). Artificially intelligent persons. Houston Law Review, 58(3), pp.537–596.

Bayern, S. (2021). Autonomous organizations. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108878203

Bayern, S., Burri, T., Grant, T.D. et al. (2017). Company law and autonomous systems: A blueprint for lawyers, entrepreneurs, and regulators. Hastings Science and Technology Law Journal, 9(2), pp.135–162.

Beckers, A. and Teubner, G. (2022). Three liability regimes for artificial intelligence: Algorithmic actants, hybrids, crowds. Oxford: Hart Publishing. https://doi.org/10.5040/9781509949373

Bryson, J.J. (2010). Robots should be slaves. In: Y. Wilks, ed. Close engagements with artificial companions: Key social, psychological, ethical and design issues. Amsterdam: John Benjamins, pp.63–74. https://doi.org/10.1075/nlp.8.11bry

Bryson, J.J., Diamantis, M.E. and Grant, T.D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. Artificial Intelligence and Law, 25(3), pp.273–291. https://doi.org/10.1007/s10506-017-9214-9

Cheong, B.C. (2024). The rise of AI avatars: Legal personhood, rights and liabilities in an evolving metaverse. Journal of Digital Technologies and Law, 2(4), pp.857–885. https://doi.org/10.21202/jdtl.2024.42

Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. International & Comparative Law Quarterly, 69(4), pp.819–844. https://doi.org/10.1017/S0020589320000366

Chopra, S. and White, L.F. (2011). A legal theory for autonomous artificial agents. Ann Arbor: University of Michigan Press. https://doi.org/10.3998/mpub.356801

Council of Europe (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Vilnius, 5 September.

Directive (EU) 2024/2853 (2024). Directive of the European Parliament and of the Council of 23 October 2024 on liability for defective products. Official Journal of the European Union, L 2024/2853.

Euronews (2026). Denmark introduces a bill protecting people's faces and voices from deepfakes. 8 October [online]. Available at: https://www.euronews.com/2026/10/08/denmark-introduces-a-bill-protecting-peoples-faces-and-voices-from-deepfakes

European Parliament (2017). Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [online]. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

Expert Group on Liability and New Technologies — New Technologies Formation (2019). Liability for artificial intelligence and other emerging digital technologies. Luxembourg: Publications Office of the European Union. https://doi.org/10.2838/573689

Floridi, L. and Taddeo, M. (2018). Romans would have denied robots legal personhood. Nature, 557, p.309. https://doi.org/10.1038/d41586-018-05154-5

IEEE (2021). IEEE Std 7001-2021. IEEE standard for transparency of autonomous systems. New York: Institute of Electrical and Electronics Engineers.

ISO/IEC (2023). ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. Geneva: International Organization for Standardization.

Kolt, N. (2025). Governing AI agents. Notre Dame Law Review, 101 (forthcoming).

Kostenko, O. (2021). Legal regulation of identity data management: UNCITRAL, cross-border trust space. Law. State. Technology, (4), pp.56–60. https://doi.org/10.32782/LST/2021-4-10

Kostenko, O. (2025). AI law model for ethical legislation: Strategic recommendations for the regulation of artificial intelligence. Calgary: SciFormat Publishing Inc. https://doi.org/10.69635/978-1-0690482-5-7

Kostenko, O. and Zhuravlov, D. (2025). Reconceptualizing jurisdiction and legal identity in the metaverse: Elements of a digital code architecture. Metaverse Science, Society and Law, 1(1) [online]. Available at: https://sciformat.ca/journals/index.php/mssl/article/view/13

Kostenko, O. et al. (2024a). «Legal personality» of artificial intelligence: Methodological problems of scientific reasoning by Ukrainian and EU experts. AI & Society, 39, pp.1683 ff.

Kostenko, O., Dniprov, O. and Zhuravlov, D. (2024b). Metaverse: Ensuring legal recognition of avatars and electronic personalities through a cross-border personalized ID-code. International Journal of Innovative Technologies in

Social Science, 2(42). https://doi.org/10.31435/rsglobal_ijitss/30062024/8141

Kurki, V.A.J. (2019). A theory of legal personhood. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198844037.001.0001

LSE Law School (2026). Dr Luke McDonagh's work cited in UK parliamentary debate on AI and digital twins [online]. Available at: https://www.lse.ac.uk/law/news/2026-09/dr-luke-mcdonaghs-work-cited-in-uk-parliamentary-debate-on-ai-and-digital-twins

Mocanu, D.M. (2022). Gradient legal personhood for AI systems — Painting continental legal shapes made to fit analytical molds. Frontiers in Robotics and AI, 8, 788179. https://doi.org/10.3389/frobt.2021.788179

NIST (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

Novelli, C. (2023). Legal personhood for the integration of AI systems in the social context: A study hypothesis. AI & Society, 38(4), pp.1347–1359. https://doi.org/10.1007/s00146-021-01384-w

Novelli, C., Bongiovanni, G. and Sartor, G. (2022). A conceptual framework for legal personality and its application to AI. Jurisprudence, 13(2), pp.194–219. https://doi.org/10.1080/20403313.2021.2010936

Novelli, C., Floridi, L., Sartor, G. and Teubner, G. (2024). AI as legal persons: Past, patterns, and prospects. SSRN Working Paper No. 5032265 (rev. 2025). https://doi.org/10.2139/ssrn.5032265

Ohio Capital Journal (n.d.). What's in Ohio's proposal banning AI personhood [online]. Available at: https://ohiocapitaljournal.com/?p=35295

Onyshchenko, N. and Kostenko, O. (2026). AI-digital human as a new class of digital law subject: Typology, criteria of legal personhood, and a registration model in digital ecosystems. Metaverse Science, Society and Law, 2(4). https://doi.org/10.69635/mssl.2026.2.4.63

Regulation (EU) 2016/679 (2016). Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119.

Regulation (EU) 2024/1183 (2024). Regulation of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union, L 2024/1183.

Regulation (EU) 2024/1689 (2024). Regulation of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.

Republic of Korea (2025). Framework Act on the Development of Artificial Intelligence and Establishment of Trust, Act No. 20676, promulgated 21 January 2025, entered into force 22 January 2026.

Science and Technology Daily (2026). New rules to regulate human-like AI interactive services. 28 July [online]. Available at: https://www.stdaily.com/web/English/2026-07/28/content_554571.html

Solum, L.B. (1992). Legal personhood for artificial intelligences. North Carolina Law Review, 70(4), pp.1231–1287.

Stone, C.D. (1972). Should trees have standing? Toward legal rights for natural objects. Southern California Law Review, 45, pp.450–501.

Teubner, G. (2018). Digital personhood? The status of autonomous software agents in private law. Ancilla Iuris, pp.106–149.