

Cristina Donia BODNARIUC*

DIGITAL PERSON AS LEGAL FICTION UNDER THE AI ACT, GDPR, AND EIDAS

This article examines how the EU's emerging regulatory triangle, Regulation (EU) 2024/1689 (the AI Act), Regulation (EU) 2016/679 (the GDPR), and Regulation (EU) 2024/1183 (eIDAS 2.0/EUDI Wallet), reconstructs the legal identity of individuals in algorithmic environments. It argues that, taken together, these instruments implicitly generate a functional legal fiction of the digital person: the composite techno-legal representation through which the natural person's rights, attributes, and vulnerabilities are mediated by credentials, data traces, profiles, and AI-assisted decisions. Drawing on Roman law's stratified concepts of persona, status, and caput and on modern theories of legal fiction, the article shows why treating AI as an autonomous legal subject would displace responsibility and fragment remedies, while treating individuals only as data subjects is normatively too thin for high-stakes digital governance. The paper proposes a twofold move, namely the normative personification of the individual in digital contexts and the use of transparent liability vehicles for certain AI systems, such as a limited electronic legal person (PJE), without ontological personality.

Keywords: digital person, legal fiction, AI Act, GDPR, eIDAS 2.0.

1. INTRODUCTION: FROM SUBJECT OF LAW TO DIGITAL PERSON

The expansion of artificial intelligence (AI) in administration, the economy and justice forces law to reconsider how it constructs the human figure to whom rights, duties and remedies attach. In increasingly digitised environments, the individual no longer appears in law as a single and stable figure, but through a layered representation composed of partial identities, electronic credentials, data trails, inferred characteristics, and AI-mediated classifications.

In European Union (EU) law, this transformation is articulated in fragmented form through three major regulatory regimes: Regulation (EU) 2024/1689 (the AI Act), Regulation (EU) 2016/679 (the GDPR) and the revised framework introduced through Regulation (EU) 2024/1183 (eIDAS 2.0/EUDI Wallet). Read separately, each of these instruments regulates a distinct field. Read together, they reveal something more important: the emergence of a legally

* Independent legal researcher (AI & Law), Guest Editor, Global Legal AI, ORCID: <https://orcid.org/0009-0000-3766-137X>, email: doniabodnariuc@gmail.com

relevant representation of the individual that cannot be reduced either to the analogue natural person or to the informational category of the data subject alone. It is this additional layer of legal representation that this article names the digital person.

1.1. Normative context: the AI Act, the GDPR, eIDAS 2.0

Regulation (EU) 2024/1689 introduces a risk-based framework for AI systems, focused on high-risk systems used in fields such as employment, education, credit, essential services, migration, law enforcement, and the administration of justice. The GDPR structures the individual as a data subject, that is, as the bearer of a bundle of rights attached to the processing of personal data. Regulation (EU) 2024/1183, by establishing the European Digital Identity Framework and the European Digital Identity Wallet, adds a further layer of legally recognized digital identification and credential management.

These instruments are not merely adjacent. A high-risk AI system used in recruitment, credit assessment or access to public services may rely on electronic identification, large-scale personal data processing and AI-assisted classification within a single socio-technical interface. The result is a stratified normative architecture in which legal identity is increasingly mediated through digital infrastructures.

1.2. Why the language of the data subject is not enough

The GDPR's concept of the data subject has been indispensable for the constitutionalization of data protection in Europe. Yet, in AI-mediated environments, it is not fully sufficient. The individual is not only the subject whose personal data are processed; they are also the subject whose eligibility, credibility, risk, capacity, and access to opportunities may be shaped by scores, labels, recommendations, and automated classifications.

By digital person I do not mean a new legal subject replacing the natural or legal person. I mean a functional legal construct through which institutions identify, authenticate, classify, evaluate and govern an individual across data-driven and AI-mediated environments. The digital person is the legally relevant composite of credentials, data traces, profiles, inferred characteristics and decision-significant representations through which rights, opportunities and vulnerabilities are increasingly mediated.

The concept should also be distinguished from adjacent notions. It is not reducible to the data subject under the GDPR, because it exceeds the mere status of a person whose personal data are processed. It is not identical with digital identity under eIDAS 2.0, because identity credentials represent only one formal layer of a broader techno-legal representation. Nor is it synonymous with a profile, avatar or online persona, because those notions remain either technical, sociological or platform-specific. The digital person is a legal-conceptual synthesis of these fragments insofar as they become operationally relevant for access, exclusion, verification, allocation and accountability.

Finally, the digital person should not be conflated with the notion of the affected person or subject of an AI system as used in the AI Act. Those notions describe a situational relationship between an individual and a specific high-risk system at a particular moment of deployment. The digital person, by contrast, names the enduring techno-legal configuration of the individual across multiple and cumulative infrastructures (credentials, data traces, profiles, inferred characteristics) that persists before, during and after any single system interaction. Where the AI Act identifies a role in relation to a system, the digital person names the legally relevant layer of representation through which that role is exercised and its effects accumulate.

What is missing in current doctrine is therefore not another metaphor for digital life, but a concept capable of capturing both the representational dimension of the person in data and credentials, and the performative dimension through which those representations produce legal and social effects. The notion of the digital person is proposed here as that missing doctrinal bridge.

1.3. Method: Roman law and the theory of legal fictions

Methodologically, the article combines historical-conceptual analysis with normative reconstruction. The first part revisits the Roman law categories of *persona*, *status* and *caput* in order to show that legal identity has never been monolithic, but has instead been structured through layered legal positions vulnerable to partial losses of status. The figure of *capitis deminutio* provides a useful matrix for thinking about contemporary forms of digital *capitis deminutio*, in which the individual retains full natural personhood while effective access to rights may nonetheless be curtailed through data-driven and credential-based infrastructures. The second part reconstructs how the AI Act, the GDPR and eIDAS 2.0 jointly configure a legal environment in which the digital person becomes visible as a practical and doctrinal necessity. The third part develops the digital person as a legal fiction and differentiates it from proposals for AI legal personhood. The fourth part relates this concept to questions of liability and institutional design, including the use of transparent legal vehicles such as the limited electronic legal person (PJE).

2. PERSONA, STATUS, CAPUT: STRATIFIED IDENTITY IN ROMAN LAW

Roman law offers a useful lens because it treated legal identity as structured through *persona*, *status* and *caput* rather than as a monolithic natural fact. A person's legal position depended on recognised statuses and could be altered without erasing the individual's presence in the legal order altogether. The figure of *capitis deminutio* is especially useful here because it captures changes in legal position through loss or alteration of status.

This offers an instructive analogy for contemporary digital environments. The individual now appears through civil, informational, electronic and algorithmic layers of representation. We can therefore speak of an extended digital *caput* vulnerable to subtle forms of digital *capitis deminutio*: a compromised identity wallet, invalidated credential, negative score or persistent algorithmic label may not erase legal personhood, but can materially restrict access to employment, services, mobility or recognition.

Roman law thus offers not a ready-made solution but a conceptual lesson: legal vulnerability may arise through partial degradation of legally relevant status, and law needs concepts capable of naming and responding to such losses.

3. THE NORMATIVE TRIANGLE OF THE DIGITAL PERSON: THE AI ACT, THE GDPR, eIDAS 2.0

3.1. The AI Act: high-risk AI systems, governance and traceability

Regulation (EU) 2024/1689 establishes the Union's general framework for AI. For the present analysis, its significance lies not only in the classification of high-risk systems, but in the fact that it identifies the institutional settings in which algorithmic processing can materially

affect a person's economic and social position: employment, education, credit, essential services, migration, law enforcement and justice. In these settings, what is acted upon is often not the embodied individual in abstraction, but the individual's digitally mediated representation – their scores, labels, histories and inferred characteristics.

The AI Act is also crucial because it translates concern for the affected person into concrete governance obligations, including risk management, data governance, technical documentation, logging, human oversight and post-market monitoring. These obligations define the conditions under which the modelling of the digital person can later be reconstructed, contested and assessed by courts or supervisory authorities (Yeung, 2018).

From this perspective, the high-risk regime can be read as a regime of enhanced legal protection for situations in which the individual's digital caput is exposed to structural harm. Where the law requires heightened traceability and oversight, it implicitly recognises that the person's opportunities, status and access to goods or services may be reshaped through algorithmic mediation.

3.2. GDPR: the data subject as informational subject of law

Regulation (EU) 2016/679 remains the backbone of the EU's framework for the processing of personal data. It defines the individual as a data subject and grants rights of information, access, rectification, erasure, portability, objection, complaint, and compensation, structured around principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, and accuracy.

The GDPR therefore supplies the informational layer of the digital person. It determines how the individual appears in databases, records and processing operations, and which forms of legal control they can exercise over that representation. At the same time, its vocabulary remains narrower than the wider legal reality of AI-mediated governance. It captures the legality of processing, but not always the full performative force of scores, labels, and classifications that condition access to work, credit, or public services.

The Court of Justice's judgment in *SCHUFA Holding (Scoring)* (2023) is especially significant in this respect, because it clarifies that the automated establishment of a credit score may amount to a decision within the meaning of Article 22 of the GDPR where a third party relies decisively on that score. The case is important not only for data protection doctrine, but because it reveals how a digitally produced representation of the person can operate as the legally decisive interface through which opportunities are granted or denied.

3.3. eIDAS 2.0: electronic identity and credentials

Regulation (EU) 2024/1183, which establishes the European Digital Identity Framework, adds another layer. Through the European Digital Identity Wallet, the individual can store, present and use electronic credentials issued by public authorities and, in certain contexts, by private actors. These may include proof of identity, age, residence, qualifications, licenses, or other attestations of legal or social status.

eIDAS 2.0 is therefore not simply about technical convenience. It reorganizes the legal presentation of the person before institutions and markets through a credential architecture capable of verifying attributes across borders and conditioning access to services on the successful presentation of legally trusted digital proofs.

3.4. Layers of identity: physical, informational, electronic, algorithmic

Read together, the AI Act, the GDPR and eIDAS 2.0 delineate at least four analytically distinct layers of legal identity. At the base stands physical and civil identity, anchored in domestic law. The GDPR structures informational identity. eIDAS 2.0 organises electronic identity through credentials and wallet-based presentation. The AI Act, finally, makes visible an algorithmic identity expressed through scores, labels, probability values, risk indicators and AI-assisted decisions.

The digital person emerges at the intersection of these layers. It is not someone other than the natural person, but the way in which the natural person is represented, verified, evaluated and acted upon within complex technical infrastructures. The normative triangle of the AI Act, the GDPR and eIDAS 2.0 thus functions as the legal matrix within which the digital person is produced.

Operationally, this matters because courts and regulatory authorities are increasingly confronted with disputes in which the central issue is not simply whether data were processed lawfully, but how the individual was rendered legible to the system and how that rendering affected access, exclusion, verification or liability. The digital person names that legally contestable interface between the human being and the socio-technical apparatus that represents, evaluates and acts upon them.

The operational significance of this intersection can be illustrated by a single scenario. Consider an AI-assisted recruitment system classified as high-risk under Annex III of the AI Act, which requires candidates to submit qualifications and identity attributes verified through the European Digital Identity Wallet under eIDAS 2.0 and generates automated eligibility scores processed under the GDPR. In such a configuration, all three instruments apply simultaneously to the same person. eIDAS 2.0 governs the presentation of credentials, the GDPR the lawfulness of processing, including safeguards under Article 22 where automated scoring produces legally significant effects, and the AI Act imposes transparency, human oversight and traceability obligations on the deployer. The natural person thus appears not as a unified legal subject, but as a composite of verified attributes, processed data, and inferred scores, a configuration that this article calls the digital person.

This convergence also reveals tensions that the concept of the digital person must capture. The AI Act's traceability and record-keeping requirements may sit uneasily with the GDPR principles of data minimisation and storage limitation, while the selective-disclosure logic encouraged by eIDAS 2.0 may narrow the informational basis for algorithmic assessment, with consequences for both accuracy and auditability. These frictions do not dissolve at the level of any single instrument.

4. THE LEGAL FICTION OF THE DIGITAL PERSON

4.1. From AI legal personhood to the digital person

Against this background, the debate on AI legal personhood appears conceptually misplaced. To attribute legal personality to AI systems on the basis of technical autonomy is to collapse two distinct planes: technical autonomy, meaning the capacity of a system to operate without continuous human intervention, and legal autonomy, meaning the capacity to hold rights and obligations in one's own name.

That collapse is normatively hazardous. It risks personifying artefacts while obscuring the human and institutional actors who design, train, deploy, oversee and profit from them. Instead of clarifying responsibility, it introduces a new fictive layer between the harmed individual and the actors who should remain legally visible.

The more coherent move is a different one: not to personify AI systems as autonomous legal subjects, but to make explicit the already emerging legal fiction through which the individual is represented and affected in digital environments. The central question is not whether AI deserves personhood, but how law should conceptualise the digitally mediated person upon whom AI systems operate.

4.2. Limits of AI legal personhood and the risks of an autonomous subject

Attempts to analogise AI with corporate legal persons are ultimately unconvincing. Corporate personhood is embedded in a dense architecture of human organisation, governance, patrimony and representation. Its fiction serves a clear institutional function. AI systems, by contrast, remain technical artefacts whose external effects depend on human choices regarding design, training data, deployment settings, monitoring and intervention.

Recognising AI as an autonomous legal subject would therefore generate at least three risks. It would displace responsibility from identifiable human and institutional actors to a fictive entity lacking moral agency; it would fragment the architecture of liability by interposing an additional layer between victims and those who benefit from the system; and it would distort the grammar of fundamental rights by suggesting a false symmetry between human persons and AI artefacts.

For these reasons, the personification of AI should be resisted. The more important task is to clarify the status of the digital person and to design transparent mechanisms through which responsibility for high-risk AI systems can be organised without ontological mystification.

4.3. The digital person as a functional fiction: rights, obligations and evidence

The digital person can be understood as a functional legal fiction. It does not claim to add a new subject to the legal order. It makes a more modest but necessary claim: that the composite techno-legal representation through which an individual is identified, evaluated and acted upon within algorithmic infrastructures has become sufficiently consequential to require legal naming. Naming that representation is the first step toward making it contestable, correctable and remediable.

The digital person can now be defined more precisely as the normative configuration of identities, credentials, data traces, profiles and inferred characteristics attributed to a natural person within legal and technical infrastructures, through which that person gains or loses access to rights, services, opportunities and protections.

This definition has several consequences. First, the digital person is derivative: it does not replace the natural person, but overlays it as a legally relevant representational layer. Second, it is infrastructural: it exists through registers, databases, identity wallets, logs, models and other technical artefacts. Third, it is performative: the way in which it is configured produces real distributive effects, because it can determine who is considered eligible, trustworthy, risky, ineligible or suspicious.

If the digital person is understood as the second legal skin of the individual in AI-data-identity infrastructures, it becomes possible to articulate a more coherent set of rights

and correlative duties. The GDPR rights can be re-read as rights of the digital person over its informational configuration. The AI Act safeguards in high-risk domains protect the person's digital caput against opaque or unjustified algorithmic mediation. eIDAS 2.0 adds control over the credential layer through which the person proves identity or status in digital form.

On the other side stand correlative obligations. Data controllers, AI providers, deployers, wallet administrators and public authorities all participate in producing and managing the digital person. Their duties should therefore be read not only as duties of technical compliance, but as duties to maintain the integrity of the person's techno-legal representation: duties of accuracy, explanation, record-keeping, traceability, contestability and remediation.

The digital person is also a probative concept in the sense that it helps identify the legally relevant site at which evidence concerning representation, categorisation and algorithmic effect must be sought. In disputes concerning algorithmic discrimination, exclusion from services, erroneous scoring, or compromised credentials, the decisive legal question is often not simply who clicked, approved, or refused, but how the person was modelled, categorized, and rendered actionable within the system. The fiction of the digital person therefore justifies enhanced requirements for logging, retention of records, auditability and procedural access to the elements through which that representation was constructed.

In judicial and regulatory practice, the concept of the digital person can serve as a structured analytical lens. Where access to employment, credit, public benefits or other essential opportunities has been shaped by data-driven or AI-assisted processing, courts and supervisory authorities should ask at least three questions: how was the person represented within the system; which legal and technical actors contributed to that representation; and which rights of access, rectification, explanation, contestation or redress are required to repair the resulting distortion or exclusion. The value of the concept lies precisely in making those questions visible as legal questions, rather than leaving them dispersed across technical subsystems.

4.4. The digital person, PJE and the architecture of liability

The digital person must finally be distinguished from, yet connected to, proposals concerning the institutional organisation of liability around AI systems. This is where the model of the PJE becomes relevant. Their functions are not the same. The digital person describes how the human person is represented and affected in digital environments. The PJE, by contrast, is conceived as a transparent legal vehicle through which responsibility for certain high-risk AI systems may be organised without treating the AI system itself as an autonomous subject.

In a coherent architecture, the PJE would operate as a container of liability: a vehicle concentrating a ring-fenced patrimony, an identified human administrator, obligations of audit and traceability, and a risk-calibrated regime of responsibility. Its point is not to emancipate AI from human control, but to make the allocation of accountability more visible and more enforceable. The doctrinal foundations and institutional architecture of the PJE have been developed in detail elsewhere (Bodnariuc, 2025a; Bodnariuc, 2025b).

The PJE draws on a Kelsenian understanding of legal personality as a technique of imputation rather than a statement of ontological fact (Kelsen, 1945, p. 93). Its function is not to say what AI is, but to create a legally intelligible point around which obligations, risk and patrimonial responsibility may be organised. Like the corporate person, the PJE is a juridical construct: it does not personify the system itself, but structures legal consequences around a designated vehicle. For that reason, it is not designed to displace the AI Act's existing compliance architecture. The

requirements applicable to high-risk AI systems remain intact, as do the actor-specific obligations imposed on providers, importers, distributors and deployers. What the PJE adds is not a substitute for that framework, but an immediately addressable liability point and an identifiable patrimony where harmful effects emerge from distributed high-risk AI operations.

As proposed here, the PJE would not operate as a general legal form for all AI systems, but as a narrowly tailored vehicle for a limited class of high-risk, operationally autonomous systems whose harmful effects may emerge through distributed chains of design, deployment and use. Its minimum constitutive elements would include a ring-fenced patrimony, a designated human administrator, duties of auditability and traceability, and a clear interface for compensation and recourse. In that sense, the PJE is not meant to symbolically personify AI, but to juridically stabilise the point at which responsibility becomes visible, enforceable and economically meaningful.

This distinction becomes even more important in the current EU landscape. The Product Liability Directive (Directive (EU) 2024/285) has now been revised so as to extend no-fault liability rules to software and other digital products, while the Commission has announced the withdrawal of the proposed AI Liability Directive because no foreseeable agreement existed on the text and it will assess whether another proposal, or another type of approach, should be tabled (European Commission, 2025). The liability debate has therefore not disappeared; it has become more fragmented and, for that very reason, conceptually more in need of a unifying account of the represented individual upon whom these regimes converge.

The model proposed here would allow for a layered liability architecture suited to that fragmented landscape. At the first level, the PJE could provide an immediate compensation interface within its ring-fenced patrimony and any attached mandatory insurance. At the second, the designated human administrator could incur subsidiary responsibility for negligent supervision, configuration or failure to intervene within authorised operational limits. At the third, recourse could extend along the wider technological chain, calibrated to the causal contribution of the designer, integrator, deployer or user. Such layering does not dilute human responsibility; it makes it visible and legally actionable where distributed operations would otherwise dissolve into evidentiary difficulty.

Within such a framework, the digital person serves as the reference point for assessing harm. When an AI-supported system affects access to work, credit, benefits or essential services, what is often harmed first is not an abstract human being in the air, but the person's digital caput: their scores, labels, statuses, credentials and machine-readable representation. The PJE, where used, would organise responsibility around the system; the digital person would identify the legally relevant site of impact.

The advantage of this separation is twofold. It preserves the centrality of the human person and their dignity, while also making room for institutional techniques capable of concentrating patrimonial risk and compliance duties around high-risk systems. The digital person and the PJE are thus not competing fictions, but complementary instruments of a legal architecture that resists AI personhood while strengthening intelligibility, contestability and effective redress.

5. CONCLUSIONS: RESISTING AI LEGAL PERSONHOOD AND STRENGTHENING THE DIGITAL PERSON

This article has argued that the emerging EU framework on AI, data protection and digital identity implicitly produces a new legal figure: the digital person. Using the Roman law

categories of persona, status and caput as a conceptual lens, it has shown that legal identity has always been stratified and that vulnerability can arise through partial losses of legally relevant status rather than only through total exclusion.

In contemporary AI-data-identity infrastructures, this stratification reappears in digital form. The individual is simultaneously a bearer of civil status, a data subject under the GDPR, a holder of electronic credentials under eIDAS 2.0 and the target of algorithmic scoring, profiling and classification under the AI Act. The digital person names the techno-legal configuration through which these layers become operational in practice.

On that basis, the article has argued that debates on AI legal personhood move in the wrong direction. To recognise AI systems as autonomous legal subjects would obscure the human and institutional actors who design, deploy and benefit from those systems. The preferable route is to make explicit the fiction that is already working beneath the surface of EU law: the digital person as the legally relevant representation of the human individual in data-driven and AI-mediated environments.

The digital person is not a competitor to the natural person, but a second legal skin around which rights, duties and evidentiary guarantees can be organised. It offers a clearer focal point for claims concerning intelligibility, rectification, contestation, traceability and effective redress. It also enables courts and regulators to treat the modelling of the person within a system as a central juridical question rather than as a merely technical background issue.

In institutional terms, the article has also suggested that the digital person can be combined with transparent liability vehicles such as the PJE. In that architecture, the PJE would organise patrimonial risk and accountability around certain high-risk AI systems, while the digital person would remain the reference point for identifying and repairing harm. Such an approach avoids ontological mystification, preserves the centrality of human dignity and fits better with the current, still fragmented, EU landscape of AI governance and liability.

Explicit recognition of the digital person would therefore provide a doctrinal bridge between AI governance, data protection, digital identity, adjudication and liability. In a legal order increasingly confronted with machine-mediated access to work, credit, welfare, justice and public services, that bridge is becoming normatively necessary.

LIST OF REFERENCES

Literature

- Bodnariuc, C. D. 2025a. De la Cicero la AI (I): Fundamente istorice si teoretice ale persoanei juridice electronice limitate. Bucharest: Universul Juridic. Available at: <https://www.universuljuridic.ro/de-la-cicero-la-ai-i-fundamente-istorice-si-teoretice-ale-persoanei-juridice-electronice-limitate/> (24. 11. 2025).
- Bodnariuc, C. D. 2025b. De la Cicero la AI (II): Necesitatea si arhitectura normativa a persoanei juridice electronice limitate. Bucharest: Universul Juridic. Available at: <https://www.universuljuridic.ro/de-la-cicero-la-ai-ii-necesitatea-si-arhitectura-normativa-a-persoanei-juridice-electronice-limitate/> (9. 12. 2025).
- Kelsen, H. 1945. *General Theory of Law and State*. Cambridge, MA: Harvard University Press.
- Yeung, K. 2018. Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), pp. 505–523. <https://doi.org/10.1111/rego.12158>

Legal sources

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, pp. 1-88.
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. OJ L, 2024/1183, 30.4.2024.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. OJ L, 2024/1689, 12.7.2024.
- Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. OJ L, 2024/2853, 18.11.2024.
- European Commission. 2025. Commission Work Programme 2025: Moving Forward Together: A Bolder, Simpler, Faster Union. COM(2025) 45 final. Brussels: European Commission. Available at: https://commission.europa.eu/publications/2025-commission-work-programme-and-annexes_en (21. 4. 2026).

Case law

- SCHUFA Holding (Scoring), 2023. CJEU, Judgment of 7 December 2023. (Case C-634/21, ECLI:EU:C:2023:957). Available at: <https://curia.europa.eu/juris/liste.jsf?num=C-634/21> (21. 4. 2026).