DIGITAL REPRESENTATION AND ITS TYPES: THEORETICAL AND PRACTICAL CHARACTERISTICS

Independent Researcher: **Pardayev Akmal Baykabulovich**
Institute for Retraining and Advanced Training of Legal Personnel
Akmalpardaev312@gmail.com

Annotation: *This part of the research analyzes the theoretical and practical foundations of digital representation as an emerging institution within civil law. The section defines digital representation as the legally recognized exercise of rights and obligations through electronic means, including identity verification systems, cryptographic signatures, and algorithmic agents. It proposes a typology consisting of three core forms: statutory digital representation, which derives from legal norms and ensures formal legitimacy; contractual digital representation, based on private agreements and autonomy of will; and automated or technical digital representation, which operates through programmed or AI-driven agents. The study highlights the interrelation between legal authority, technological reliability, and accountability mechanisms in each form. It also stresses the practical significance of balancing efficiency with data protection, security, and legal certainty. Drawing on both international experiences (such as the EU eIDAS Regulation and Estonia's e-Residency system) and the national context of Uzbekistan, the research demonstrates that digital representation is not merely a technical convenience but a fundamental legal evolution requiring adaptive legislation and coherent regulation.*

Keywords: *Digital representation; electronic identity; eIDAS Regulation; digital signature; automated agency; contractual delegation; civil law; Uzbekistan; legal technology; smart contracts.*

The advent of pervasive digital infrastructures has required legal systems to reconceptualize the classical institution of representation so that it functions reliably in electronic environments. Digital representation may be characterized as the set of legal and technical arrangements through which a person's rights and duties are exercised or effected via electronic means on their behalf. Unlike traditional representation, which presumes a human intermediary and physical documentation, digital representation relies on mechanisms of electronic identity verification, cryptographic authentication, platform-mediated authorizations and, increasingly, algorithmic agents. These elements jointly determine whether an action performed in cyberspace can be attributed to an identified principal and thus produce legal consequences.

At its core, digital representation involves three interdependent components: the origin of authority (statutory allocation, contractual delegation, or technical design), the means

that establish identity and consent (for example, electronic signatures and identity tokens), and the modalities of implementation (human-controlled agents, platform actions, or automated code). Legal analysis of each component must address distinct questions: by what rule does authority arise; how is the principal's assent reliably established and evidenced; and which legal rules govern faults, excesses of authority and remedies when representations fail or produce harm. A useful practical classification distinguishes three principal types of digital representation: (1) statutory or legally conferred representation, (2) agreement-based or contractual representation, and (3) automated or technical representation. Each type has characteristic legal consequences and regulatory implications.

❖ **Statutory digital representation** is grounded in law or public regulation. Under this model, certain digital acts or interactions are afforded legal effect by virtue of statute or administrative regulation. Examples include state-operated identity frameworks that authorize public bodies to act on behalf of citizens within prescribed limits, or regulations granting legal equivalence to certain forms of electronic attestation. The principal advantage of statutory solutions is uniformity and predictability: the state prescribes authentication protocols and legal consequences, removing ambiguity in cross-institutional interactions. Yet statutory systems must also manage privacy, data protection and cross-border recognition challenges.

❖ **Contractual digital representation** stems from the autonomous agreement of private parties. Here, a person expressly authorizes a platform, service provider or another person to perform specified actions on their behalf, often through terms of service, electronic mandates or digitally executed power-of-attorney instruments. This model preserves party autonomy and flexibility: delegations can be narrowly tailored and time-limited. However, contractual delegation intensifies the need for clear allocation of responsibilities and liabilities in user agreements and for transparent consent mechanisms that are intelligible to non-expert users.

❖ **Automated or technical digital representation** encompasses algorithm-driven agents and code-based executors that operate with varying degrees of autonomy. Smart contracts on distributed ledgers and AI agents that act within preset constraints exemplify this type. Automation promises speed and determinism in transactional processes, but it simultaneously complicates traditional legal categories: what constitutes intent when an autonomous program executes instructions; how to correct or reverse transactions triggered by erroneous code; and how to apportion liability between software developers, platform operators, and end users. Effective legal frameworks therefore need to combine ex ante technical standards with ex post remedial mechanisms.

From a practical perspective, the diffusion of digital representation yields tangible benefits including streamlined administrative procedures, faster commercial transactions, and reduced reliance on paper-based bureaucracy. National implementations of unified identity services and trusted-signature regimes illustrate how technical and legal

instruments can be synchronized to enable routine electronic representation. Nevertheless, several risks persist: identity compromise, unauthorized delegation, opaque decision-making by algorithmic agents, and cross-jurisdictional recognition failures. Addressing these risks requires layered safeguards — robust identity assurance, tamper-evident audit logs, clear contractual terms, and legal rules that enable effective redress. In assessing regulatory priorities, policymakers should pursue a balanced strategy. First, they ought to adopt interoperable identity and trust-service standards that facilitate legal recognition while protecting personal data. Second, contractual transparency and user-centric consent procedures should be mandated to reduce asymmetries of information in platform-based delegations. Third, regulators must develop norms governing automated agents, including liability allocation, mandatory logging of decision parameters and mechanisms for transaction reversal where feasible. Finally, comparative study of different national systems offers valuable lessons: states that combine strong technical identity frameworks with clear legal recognition tend to achieve higher user trust and wider adoption of digital representation tools.

To conclude, digital representation is not merely a technical convenience: it reconfigures foundational legal concepts such as agency, assent and attribution. A typology that separates statutory, contractual and automated forms provides a practical scaffold for legal analysis and rule-making. As digital ecosystems evolve, legal regimes must adapt by codifying interoperable identity protocols, ensuring contractual clarity, and creating accountability mechanisms suitable for automated actors, thereby preserving legal certainty while harnessing the efficiencies of digital mediation.

REFERENCE

1. Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. Duke Law Journal, 67(2), 313–382. https://scholarship.law.duke.edu/dlj/vol67/iss2/2 (scholarship.law.duke.edu)
2. Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contract templates: Foundations, design landscape and research directions. arXiv. https://arxiv.org/abs/1608.00771 (policyreview.info)
3. Corrales Compagnucci, M., Fenwick, M., & Wrbka, S. (Eds.). (2021). Smart Contracts: Technological, Business and Legal Perspectives. Hart Publishing. (bloomsbury.com)
4. Koulu, R. (2024). In search of living law: How should we design for interaction in material-digital legal environments? Law & Critique. Advance online. https://doi.org/10.1007/s44206-024-00117-y (SpringerLink)
5. Cambridge Centre for Alternative Finance. (n.d.). Legal and regulatory considerations for digital assets. University of Cambridge Judge Business School. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-

finance/publications/legal-and-regulatory-considerations-for-digital-assets/ (Cambridge Judge Business School)

6. MyGov Uzbekistan. (n.d.). Unified Interactive Government Services Portal. https://my.gov.uz/en (Cambridge Judge Business School)

7. e-Estonia. (n.d.). e-Residency. https://e-estonia.com/solutions/estonian-e-identity/e-residency/ (bloomsbury.com)

8. European Parliament & Council. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2014/910/oj (EU Data Act)

9. Law of the Republic of Uzbekistan "On Electronic Digital Signature" No. 562-II, 11 December 2003. (2003). Lex.Uz. https://www.lex.uz/docs/4410899 (scholarship.law.duke.edu)