LEGAL AND ADMINISTRATIVE STUDIES, www.jlas.upit.ro.
e-ISSN: 2344-6900, ISSN-L: 1583-0772
No.2 (33), Year XXIV, 2025, pp. 9-27

RE-ENGINEERING SOCIETY: LEGAL, INSTITUTIONAL, AND TECHNOLOGICAL DIMENSIONS OF DIGITAL TRANSFORMATION

Giorgi KHARSHILADZE
ORCID ^{ID}: 0000-0002-8357-5525
E-mail: gkharshiladze@thu.edu.ge
Afiliation: Tbilisi Humanitarian University, Georgia
Faculty of Law, Business, Humanities, and Social Sciences

Abstract: *Digital transformation is a multifaceted process that reconfigures social, economic, institutional, and legal structures through the diffusion of information and communication technologies. This paper examines digital transformation as a process of societal re-engineering by integrating three analytical lenses: legal and regulatory frameworks, institutional and governance change, and technological foundations and socio-economic outcomes. Drawing on established scholarship in surveillance capitalism, network society theory, and economic analyses of digital technologies, as well as contemporary regulatory developments (notably the EU General Data Protection Regulation and the EU Artificial Intelligence Act), the study maps how legal norms, institutional capacities, and core technologies interact producing novel risks and opportunities. The analysis emphasizes tensions between innovation and rights protection, the necessity of interoperability and institutional redesign for public sector digitalization, and the distributional effects of automation and platformization on labor and markets. The paper concludes with policy recommendations for balanced regulatory design, capacity building in public institutions, and ethical governance mechanisms to steer digital transformation toward social resilience and democratic accountability.*

Keywords: *Societal re-engineering; legald and regulatory frameworks; Institutional Governance; Emergic Technologies and Public Policy.*

Introduction

Digital transformation has emerged as one of the defining structural processes of the twenty-first century, reshaping how societies organize production, communication, governance, and everyday life. While digitalization has long been associated with efficiency, modernization, and innovation, contemporary scholarship demonstrates that the transformation underway goes beyond the deployment of isolated technologies. It entails a fundamental re-engineering of societal systems through datafication - the systematic conversion of behavior, relationships, and institutional processes into data - as well as through rapid advancements in computation, network connectivity, artificial intelligence (AI), and digital infrastructures.

The conceptual foundations of this shift have been articulated across multiple disciplinary traditions. Manuel Castells' theorization of network society illustrates how information flows reorganize social structures and spatial relations: in his work, power no longer concentrates in territorial states alone, but in actors who control data networks and information infrastructure (Castels, 2010, pp.28-45). Complementing this perspective, Shoshana Zuboff's analysis of surveillance capitalism highlights a new economic logic in which platforms accumulate behavioral data and convert it into predictive and commercial value, thereby transforming citizen–platform relations and political economy (Zuboff, 2019, pp. 1-2, 111, 376).

Economic analyses by Erik Brynjolfsson and Andrew McAfee further illuminate the impact of digital technologies on labor and growth. In „The Second Machine Age", they argue that automation, intelligent systems, and networked infrastructure are reshaping productivity, employment, and what it means to work in the information age (Brynjolfsson, & McAfee, 2014, pp. 81-103, 167-176).

Beyond these foundational works, more recent research underscores how digital transformation is not only theoretical but deeply practical and urgent. For instance, the OECD's 2025 report „Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions" argues that AI is accelerating digital-government trajectories and demanding new governance models. The report proposes that states integrate AI into regulatory design and public service delivery, while ensuring safeguards and transparency[1].

At the same time, normative scholarship is grappling with the ethics of AI and regulation. Manuel Woersdoerfer suggests an “Ordoliberal 2.0” framework in his paper „AI Ethics and Ordoliberalism 2.0: Towards a ‘Digital Bill of Rights“, arguing that ethical principles and competition policy should merge to form a robust digital rights architecture (Woersdoerfer, 2023). Scholarly work further stresses the need for institutional structures that can implement and enforce AI regulation: Claudio Novelli, Phillipp Hacker, Jessica Morley, Jarle Trondal, and Lucciano Floridi propose a governance model for the EU AI Act that includes a dedicated “AI Office,” a European AI Board, and a scientific panel to supervise risk and coordinate national authorities (Novelli, Hacker, Morley, Trondal, and Floridi, 2023).

Empirical and normative studies also highlight the global dimension of AI governance. Jonas Tallberg, Eva Erman, Markus Furendal, Joannes Geith, Mark Klamberg, and Marcus Lundgren in „The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research“ argue for a dual research agenda: one that maps power relations in global AI governance and one that formulates universal principles suited to emergent regulatory architectures (Tallberg, Erman, Furendal, Geith, Klamberg, and Lundgren, 2023). Public opinion research provides complementary insight: Justin B. Bullock, Janet V.T. Pauketat, Hsini Huang, Yi-Fan Wang, and Jacy Reese Anthis examine trust, risk perception, and public support for AI regulation in their survey-based study „Public Opinion and The Rise of Digital Minds“. They find that trust in institutions strongly influences regulatory preferences, underscoring that governance must respond not only to

[1] OECD. *How artificial intelligence is accelerating the digital government journey*.

technological risk, but also to societal sentiment (Bullock, Pauketat, Huang, Wang, and Anthis, 2025).[1]

On the regulatory front, numerous new laws and policy proposals reflect how the digital transformation is being actively shaped. The „European Union's Data Act“ (Regulation (EU) 2023/2854) establishes rules for fair access to and use of data, aiming to foster data-driven innovation while protecting rights The „Cyber Resilience Act“ (Regulation (EU) 2024/2847) further embeds security requirements for products with digital elements, integrating cybersecurity more deeply into the regulatory fabric. Meanwhile, strong new requirements for financial entities are emerging under the „Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554)“, which mandates ICT risk management, digital resilience, and third-party oversight in the financial sector.

Scholars studying AI regulation also emphasize the importance of trust and social risks. In an review „Building Trust in the Generative AI Era: A Systematic Review of Global Regulatory Frameworks“, researchers highlight how misinformation, disinformation, and malinformation (MDM) produced by generative AI necessitate regulatory mechanisms that protect public discourse, transparency, and accountability (Abbas, Chesterman, and Taeihagh).[2]

As digital infrastructures evolve, so too do the legal, institutional, and ethical challenges. The transformation demands not only new laws, but also capable institutions and normative frameworks that align innovation with social values.

[1] Examine trust, risk perception, and public support for AI regulation in their survey-based study „Public Opinion and The Rise of Digital Minds“. (2025).

[2] Fakhar Abbas, Simon Chesterman, Araz Taeihagh - Building trust in the generative AI era: a systematic review of global regulatory frameworks to combat the risks of mis-, dis-, and mal-information.

Legal and Regulatory Foundations of Digital Transformations

Digital transformation deeply reshapes legal regimes by converting social behavior into data, demanding new normative frameworks that reconcile individual rights with technological innovation. As information becomes the backbone of economic and governance processes, traditional legal categories — such as fault liability, territorial jurisdiction, and administrative oversight — face profound tests. The ubiquity of data collection, automation, and algorithmic decision-making creates regulatory pressure to reinterpret fundamental legal principles and design new mechanisms for accountability (Novelli, Hacker, Morley, Trondal and Floridi, 2024, pp. 3-7).

At the heart of data regulation lies the European Union's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which establishes a rights-based approach to personal data protection. The GDPR enshrines principles — lawfulness, fairness, transparency, purpose limitation, and data minimization — that bind data controllers and processors[1]. Furthermore, it guarantees data subject rights such as access (Art. 15), rectification (Art. 16), erasure (Art. 17), objection (Art. 21), and portability (Art. 20). Organizations are required to implement technical and organizational measures, such as data protection by design and data protection impact assessments, under the supervision of Data Protection Authorities (GDPR, 2016, Art. 35). These provisions aim to embed privacy not just as a legal restriction but as a structural feature of digital systems.

However, implementing privacy protections in automated environments is not straightforward. In algorithmic systems, obtaining meaningful consent is complicated by the opacity of processing

[1] European Union. *General Data Protection Regulation GDPR*. (2016). https://gdpr.eu.org/full/full.pdf?

pipelines, especially in machine-learning models. Moreover, the allocation of liability for harms caused by automated decision-making provokes debate: should accountability rest with the model's developer, its deployer, or the data subject? Scholars argue that legal doctrine must evolve, integrating technical standards like explainability, logging, and audit trails to enable accountability in these contexts (Yeung, 2018, pp. 505-523).

Another critical dimension of regulation arises from platform power. Digital platforms operate as gatekeepers to markets and data. Their control over multi-sided relationships (users, advertisers, service providers) leads to concentration of power and raises competition concerns. The EU Digital Markets Act (DMA) addresses such issues, imposing obligations on "gatekeeper" platforms to ensure interoperability, non-discrimination, and transparency in their business practices.[1] Importantly, these regulatory obligations reflect a shift from ex post competition enforcement to a more proactive stance, recognizing the unique market dynamics of digital ecosystems.

Artificial Intelligence (AI) introduces yet more complexity. Autonomous systems, driven by large datasets and complex algorithms, challenge legal norms around liability, safety, and trust. To mitigate these risks, the AI Act (Regulation (EU) 2024/1689) establishes a risk-based regulatory framework. Under this Act, high-risk AI systems — such as biometric identification, critical infrastructure, and public administration AI — are subject to rigorous requirements: data governance, human oversight, transparency documentation, conformity assessments, and post-market monitoring. This risk-based architecture attempts to balance innovation with protection of fundamental rights and public interest.

To ensure enforceability, the AI Act also creates governance bodies, including an AI Office and a European AI Board, which coordinate national authorities and provide technical and ethical

[1] European Union. *Digital Market Act.* https://digital-marketsact.ec.europa.eu/legislation_en?

oversight (Novelli, Hacker, Morley, Trondal, and Floridi, 2023, pp. 15-20). Such institutions are crucial for translating regulatory standards into technical compliance and for addressing cross-border challenges, given that AI systems often operate globally.

Cybersecurity is another pillar of regulation within digital transformation. As essential services, public institutions, and private platforms rely increasingly on digital systems, the threat landscape expands. The EU NIS2 Directive mandates that operators of essential and digital services adopt risk-management strategies, conduct incident reporting, and implement resilience measures. Legal requirements are complemented by institutional capacity-building: public authorities must develop cyber-risk governance, cooperation mechanisms, and continuous supervision.

Legal fragmentation across jurisdictions is a persistent challenge. Data flows, cloud infrastructure, and AI systems often transcend national borders, raising issues of cross-jurisdictional enforcement, regulatory arbitrage, and normative divergence. The GDPR's extraterritorial scope already reflects this reality, but the diversity of national AI policies and cybersecurity laws demands cooperative frameworks and standard-setting at the international level (Novelli, Hacker, Morley, Trondal, and Floridi, 2023, pp. 8-12).

Institutional and Governance Transformation

Digital transformation does not merely upgrade administrative tools, it fundamentally reconfigures the architecture, capacities, and logic of governance institutions. As scholars emphasize, technology-driven reforms such as e-government, interoperability infrastructures, algorithmic decision-making systems, and digital identity frameworks for producing a new mode of public authority — one increasingly dependent on data flows, technical standar

ds, and cross-sector coordination (Margetts, and Dunleavy, 2013, pp. 12–19). The transition from paper-based bureaucracies to digitally networked administrations alter how states perceive problems, organize resources, and exercise power. This institutional restructuring generates both efficiency gains and new vulnerabilities, requiring careful design to ensure that innovation does not erode public accountability.

Across OECD and UN member states, digital government strategies highlight several foundational pillars: interoperability, data governance, digital identity, cybersecurity, and administrative capacity-building. These pillars collectively form what is called a “digital-ready state” — an institutional ecosystem capable of orchestrating digital public services, regulating platform power, and protecting fundamental rights. Interoperability frameworks, for example, enable seamless communication among ministries, agencies, and municipalities by standardizing metadata, APIs, and registry systems. Without such standards, digital transformation becomes fragmented, producing isolated digital services that replicate bureaucratic silos in new technical form.

Digital identity systems further exemplify the deep institutional consequences of technological innovation. Estonia’s X-Road, often cited as a global benchmark, demonstrates how secure digital identity credentials allow citizens and firms to authenticate themselves across the entire public administration, simplifying interactions while strengthening traceability and audit trails. Scholars note, however, that digital identity systems shift power relations by concentrating sensitive personal data under state or quasi-state control, requiring strong legal frameworks to ensure proportionality and prevent function creep. As more public services migrate online, digital identity becomes a critical gatekeeper, raising concerns about inclusion, particularly for marginalized populations with limited digital literacy or access.

Algorithmic systems adopted by public administrations introduce additional governance complexities. Machine-learning models used for welfare allocation, predictive policing, tax fraud detection, or social risk scoring alter decision-making processes that historically relied on human discretion. Scholars warn that algorithmic governance may reinforce existing social inequalities when training data reflect historical biases. Furthermore, the opacity of algorithmic reasoning challenges traditional accountability institutions — courts, ombudsmen, audit offices — which depend on the ability to reconstruct the rationale behind administrative decisions. To address these challenges, governance bodies increasingly emphasize explainability, algorithmic auditing, and human-in-the-loop controls as prerequisites for deploying high-impact administrative AI.

Institutional transformation is also shaped by organizational culture. Public administrations traditionally value procedural stability, predictability, and hierarchical control. Digital transformation instead requires adaptability, cross-disciplinary collaboration, and iterative problem-solving. This cultural clash often slows reform. Studies of digital government efforts in the UK, Australia, and Denmark reveal that reforms succeed not merely because of new technologies but because political leadership invests in skills development, cross-agency coordination, and long-term capacity building. The transition toward digital public governance thus requires a redefinition of bureaucratic professionalism to incorporate data analytics, cybersecurity competence, and technological fluency.

Another major institutional challenge is the governance of data as a strategic public resource. As states accumulate vast administrative datasets — taxation, health, education, mobility, social services — questions arise about access, stewardship, reuse, and data-sharing. The European Union’s Data Governance Act (DGA) and the broader European Strategy for Data attempt to establish a framework for trusted reuse of public-sector data, including through data intermediaries, secure processing environments, and harmonized data-space architectures. These initiatives reflect a shift toward treating data as a public infrastructure, not merely an administrative byproduct.

Cross-sector collaboration further underscores institutional transformation. Governments increasingly rely on private technology companies to deliver digital infrastructure, cloud services, cybersecurity capabilities, and AI systems. This reliance raises issues of vendor lock-in, procurement transparency, and sovereignty over critical infrastructure. The European Court of Auditors has warned that excessive dependence on major cloud providers may jeopardize strategic autonomy and long-term resilience, urging stronger procurement rules and multi-cloud strategies. As a result, digital transformation requires the state not only to modernize internally but also to renegotiate its relationship with powerful private actors.

Institutional redesign must also account for democratic legitimacy. Digital transformation can enhance transparency and participation through open data portals, online consultations, deliberation platforms, and digital civic tools. However, these benefits materialize only when participation mechanisms are genuinely inclusive and when public institutions commit to integrating citizen input into decision-making processes. Scholars caution that digital platforms may privilege already empowered groups, amplifying inequalities in political voice unless counterbalanced by proactive inclusion measures. Thus, institutional transformation must be democratic by design, not merely technologically advanced.

Technological Infrastructures and Socio-Economic Impact

Technological infrastructures constitute the deep architecture of digital transformation, shaping not only the technical possibilities of connectivity, computation, and automation but also the distribution of economic opportunities, risks, and power within society. These infrastructures — cloud computing systems, artificial intelligence models, IoT ecosystems, data centers, broadband networks, cybersecurity frameworks, blockchain-based systems, and platform architectures — form a layered techno-institutional environment in which contemporary socio-economic life unfolds. Because these infrastructures mediate value creation, allocate computational resources, and enable new forms of surveillance and coordination, they function as political-economic institutions as much as technical systems. The socio-economic consequences of digital transformation therefore cannot be understood without situating technological infrastructures as active determinants of labor markets, corporate concentration, public governance capacities, and distributive justice.

At the foundation of the digital economy lies cloud computing, which has redefined how computation is provisioned and scaled across sectors. Hyper-scalers such as Amazon Web Services, Microsoft Azure, and Google Cloud control the bulk of the global cloud infrastructure, providing elastic computing power, storage, and AI toolchains to corporations, governments, and academic institutions. This centralization accelerates innovation by reducing entry barriers for firms that would previously require massive capital investment in IT infrastructure. Yet at the same time, it creates unprecedented concentration of structural power: dependency on a small number of providers can limit national digital sovereignty, constrain public-sector oversight capacities, and produce cascading risks. Outages in cloud systems — whether caused by misconfigurations, cyberattacks, or supply-chain vulnerabilities in microprocessor manufacturing — have immediate macro-economic ramifications, halting payment systems, logistics operations, online public services, or healthcare systems. As scholars in infrastructure studies emphasize, when a resource becomes infrastructural, its failure becomes catastrophic, not merely inconvenient. Cloud infrastructures thus represent "critical dependencies" whose vulnerabilities map directly onto socio-economic insecurity.

Artificial Intelligence — especially machine-learning models trained on large-scale datasets — constitutes the computational layer that increasingly automates decision-making across sectors. AI transforms socio-economic dynamics not because it "replaces" human labor in a simplistic sense, but because it reorganizes tasks, workflows, and value chains. Task-based analyses demonstrate that AI-driven automation displaces routine cognitive and manual tasks while creating new categories of complementary tasks requiring problem-solving, oversight, and technical creativity. Empirically, the displacement effects are concentrated among mid-skill routine jobs, contributing to labor-market polarization: growth at the high-skill and low-skill ends with erosion of the middle. The socio-economic impact therefore depends heavily on whether institutions invest in upskilling, retraining, and inclusive access to digital competencies. Without such interventions, AI tends to amplify inequality, rewarding firms and workers who can leverage computational scale while marginalizing others.

AI’s role in socio-economic governance extends beyond the workplace. Algorithmic systems increasingly mediate access to credit, employment, education, housing, healthcare, social benefits, and online visibility. Credit-scoring models determine who receives loans and at what cost; automated hiring systems filter applicants; predictive analytics guide policing and welfare allocation; recommender systems shape political discourse and consumer behavior. In these contexts, infrastructural opacity becomes a mechanism of power: affected individuals cannot meaningfully challenge decisions made by black-box systems, and even state regulators may lack the expertise or access required to audit models trained on proprietary data. As a result, AI infrastructures become de facto rule-making institutions, producing distributional outcomes outside traditional democratic accountability structures.

Another pillar of digital transformation is the Internet of Things — a vast, heterogeneous mesh of connected devices embedded in homes, factories, transport systems, and public spaces. IoT systems extend computation into everyday objects, enabling real-time monitoring, automated responses, and fine-grained data collection. In industrial contexts (Industry 4.0), IoT supports predictive maintenance, robotic coordination, and optimized supply chains; in urban contexts, IoT sensors govern traffic systems, energy grids, and environmental monitoring; in households, smart devices mediate daily routines. The socio-economic implications stem from both the value IoT generates — through efficiency and new services — and the risks it introduces. Because IoT devices often lack robust security hardening and long-term patching mechanisms, vulnerabilities at the device level can propagate through networks, enabling large-scale botnets, critical infrastructure breaches, or personal surveillance. Thus, IoT infrastructure demonstrates the paradox of digital transformation: the more interconnected systems become, the more fragile the entire socio-economic ecosystem becomes in the face of cyber threats.

Cybersecurity, therefore, is not a peripheral technical concern but an essential socio-economic infrastructure. Modern economies depend on secure digital environments for banking, energy distribution, transportation, communications, and public services. Cyberattacks on hospitals have delayed surgeries and endangered patients; ransomware targeting municipal systems has disrupted power grids and water supplies; attacks on global logistics companies have produced billions of dollars in economic losses. Because malicious actors exploit both technical vulnerabilities and geopolitical tensions, cybersecurity becomes a domain where economic resilience, national security, and individual rights intersect. Investment in cybersecurity capacity — incident response teams, standards-based procurement, secure-by-design architectures, and cross-border coordination — becomes a public good, yet one that is unevenly distributed across countries and institutions. The socio-economic cost of inadequate cybersecurity disproportionately affects small businesses, local governments, and low-income populations, who lack resources to recover from disruptions.

Platform infrastructures — digital environments that mediate interactions between users, producers, advertisers, and third-party developers — represent another central determinant of socio-economic impact. Platforms such as Amazon, Google, Meta, Alibaba, and Uber act as gatekeepers, controlling visibility, transaction flows, and data access. Network effects consolidate market power: as more users join a platform, the value of participation increases, creating high barriers to entry for competitors. The consequences include winner-take-most markets, asymmetries in bargaining power, and extraction of economic rents from smaller businesses and workers. Gig workers depend on opaque algorithmic management systems that allocate tasks, set prices, and evaluate performance without meaningful transparency or recourse. Sellers on e-commerce platforms face shifting fees, unpredictable search rankings, and data asymmetries. As scholars of political economy argue, platform infrastructures reshape capitalism by centralizing control over digital marketplaces and data flows, enabling new forms of economic domination.

Blockchain and distributed ledger technologies (DLT) offer alternative infrastructural models by decentralizing record-keeping and verification. While often associated with volatile cryptocurrency markets, blockchain's socio-economic potentials extend to supply-chain verification, digital identity systems, cross-border payments, and decentralized governance. Yet these technologies face scalability, security, and regulatory challenges. Proof-of-work systems impose high energy costs; permissionless networks complicate compliance with financial and data-protection laws; permissioned networks require governance structures that often replicate traditional hierarchies. Thus, the transformative potential of DLT depends not only on technical design but on institutional adoption, regulatory clarity, and alignment with broader economic incentives.

Data — the foundational commodity of digital transformation — flows through all these infrastructures, generating both value and vulnerability. The extraction, aggregation, and monetization of behavioral data underpin advertising ecosystems, recommendation engines, and predictive analytics. Zuboff's analysis of surveillance capitalism highlights how this process creates behavioral surplus that fuels profit-making but erodes privacy, autonomy, and democratic life. Data asymmetries concentrate knowledge and influence within a few corporations, granting them unparalleled capacity to shape information environments, market trends, and consumer behavior. The socio-economic implications include manipulation of purchasing and voting choices, differential pricing, and reinforcement of existing inequalities through algorithmic profiling. These harms disproportionately affect marginalized groups, whose data are often over-collected, under-protected, and used in ways that exacerbate vulnerabilities.

Digital divides remain one of the most persistent socio-economic consequences of technological transformation. Access to connectivity, devices, and digital skills varies dramatically across income groups, regions, and countries. Even when connectivity is available, meaningful use — the ability to leverage digital tools to improve education, health, employment, and civic participation — requires competencies and institutional support that many communities lack. The World Bank and OECD note that digital transformation can widen inequalities if policies do not address infrastructure investment, affordability, skills development, and inclusive governance. Digital divides also manifest in cloud access, AI research capacity, cybersecurity readiness, and ability to comply with regulatory standards. In effect, inequality becomes infrastructural: societies with weak technological foundations face structural disadvantages in the global digital economy.

To ensure that technological infrastructures generate inclusive socio-economic outcomes rather than exacerbating inequalities, policy interventions must operate across multiple layers. Competition policy should address data monopolies and enforce interoperability; labor-market policies must support upskilling and equitable transitions; cybersecurity regulations should mandate secure-by-design practices; public institutions need capabilities to audit AI and govern data responsibly; and social policies must buffer individuals and communities against transitional shocks. Moreover, governments may require public or sovereign cloud options to reduce dependency on foreign platforms, ensure data protection, and maintain strategic autonomy. International cooperation is essential for managing cross-border data flows, harmonizing standards, and coordinating responses to cyber threats.

Ultimately, technological infrastructures are not merely technical artifacts but socio-economic institutions that shape the distribution of power, wealth, opportunity, and risk. Whether digital transformation produces prosperity or precarity depends on how societies design, regulate, and democratize these infrastructures. Embedding equity, accountability, and resilience into technological foundations is therefore not an optional ethical add-on but a structural requirement for sustainable digital futures.

Conclusions

The contemporary wave of digital transformation represents a structural reconfiguration of social, economic, legal, and institutional orders rather than a merely technological shift. As demonstrated throughout this study, digital transformation redistributes authority, redefines institutional capacities, and reorganizes socio-economic life through the pervasive integration of data infrastructures, algorithmic systems, and automated decision-making environments. These developments challenge long-standing governance paradigms while simultaneously generating new forms of institutional dependency on technological infrastructures operated by both public and private actors.

At the legal level, digital transformation exposes the inadequacy of traditional regulatory frameworks built for analogue processes. Emerging issues such as algorithmic accountability, digital rights, data governance, privacy protection, and platform power reveal persistent mismatches between inherited legal instruments and the operational logic of automated, data-intensive systems. As the analysis of scholarly literature has shown, law is increasingly expected to function not only as a constraint but as a co-architect of digital infrastructures—tasked with designing oversight mechanisms, enabling trustworthy data ecosystems, and embedding normative safeguards directly into technological systems. This shift underscores the emergence of a *techno-legal constitution* that governs socio-technical interactions in digital societies.

Institutionally, states are confronted with a dual imperative: modernize internal capacities to manage data-driven governance, and renegotiate their position within global technological hierarchies dominated by large cloud providers and artificial intelligence platforms. Public institutions that fail to adapt risk losing operational effectiveness, regulatory sovereignty, and strategic autonomy. Conversely, those that strategically reorganize their governance models—embracing data-centric administration, interoperable infrastructures, and digital foresight—gain the ability to shape the trajectory of societal transformation rather than merely react to it.

From a socio-economic perspective, digital transformation both creates opportunities and amplifies systemic risks. While data economies and automated production systems increase productivity and facilitate new forms of value creation, they also generate deep asymmetries in access to digital resources, institutional capacity, and technological literacy. These asymmetries threaten to widen inequality across and within societies. The literature further shows that algorithmic systems, if left unregulated, may reproduce historical inequalities and embed biases into decision-making processes at scale. As such, the socio-economic consequences of digital transformation must be understood not as unintended side effects but as structurally embedded outcomes of the infrastructures themselves.

Taken together, the findings of this study clarify that digital transformation is neither neutral nor self-correcting. It is a contested political, institutional, and normative process whose outcomes depend on the design of legal frameworks, the strategic direction of governance reforms, and the societal capacity to critically shape technological infrastructures. The overall trajectory suggests that the future of digital societies will be determined less by technological innovation per se and more by the ability of institutions—and the legal systems underpinning them—to impose democratic, ethical, and accountable structures upon rapidly evolving socio-technical environments.

Therefore, the central conclusion of this research is that the re-engineering of society through digital transformation must be approached as a coordinated project involving law, institutions, and technology in mutually constitutive ways. Only through integrated governance frameworks, rights-protective regulatory models, and transparent technological infrastructures can societies ensure that digital transformation produces equitable, resilient, and human-centered outcomes. The challenge, then, is not merely to adopt new technologies but to cultivate the institutional and normative foundations necessary to sustain democratic life in an increasingly digital world.

References

Abbas, F., Chesterman, S., and Taeihagh, A. (2025). Building trust in the generative AI era: a systematic review of global regulatory frameworks to combat the risks of mis-, dis-, and mal-information. https://link.springer.com/article/10.1007/s00146-025-02698-9?

Acemoglu, D., Restrepo, P. (2019). Automation and New Tasks: How Technology Displaces and Reinstates Labor. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3390283&

Agrawal, A., Gans, J., Goldfarb, A. (2019). The Economics of Artifi cial Intelligence. https://economics.mit.edu/sites/default/files/publications/Artificial%20Intelligence%2C%20Automation%2C%20and%20Work.pdf

Bovens, M., and Zouridis, S. (2022). How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control. https://onlinelibrary.wiley.com/doi/abs/10.1111/0033-3352.00168

Bullock, J. B., Pauketat, J. V.T., Huang, H., Wang, Y.-F., and Anthis, J.R. (2025). *Public Opinion and The Rise of Digital Minds*.

Castels, M. (2010). *The Rise of Network Society. Second edition with new preface*.

European Commission. *The Geopolitics of Cloud Computing: How State-Firm Interactions Shape the Geography of Computation to Produce Digital Sovereignty and Dependence.*

European Data Protection Supervisor (EDPS). Annual Report 2022. https://www.edps.europa.eu/_en

European Parliament. (2025). REPORT on European technological sovereignty and digital infrastructure, report. https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

European Union. (2016). General Data Protection Regulation (GDPR). https://gdpr.eu.org/full/full.pdf?

European Union. Digital Market Act. https://digital-markets-act.ec.europa.eu/legislation_en?

European Union’s AI Act Regulation (EU) 2024/1689. https://op.europa.eu/en/publication-detail/-/publication/d79f3e5d-41bc-11f0-b9f2-01aa75ed71a1

Margetts, H., and Dunleavy, P. (2013). *The Second Wave of Digital Era Governance.*

Novelli, C., Hacker, P., Morley, J., Trondal, J. & Floridi, L. (2024). *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities.*

Novelli, C., Hacker, P., Morley, J., Trondal, J. and Floridi, L. (2023). *A*

Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities.

OECD. A Data-Driven Public Sector: Enabling Strategic Use of Data. https://www.oecd.org/en/publications/a-data-driven-public-sector_09ab162c-en.html?

OECD Digital Governance Studies. The E-Leaders Handbook on the Governance of Digital Government. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/12/the-e-leaders-handbook-on-the-governance-of-digital-government_2523ea2c/ac7f2531-en.pdf?

OECD. (2025). How artificial intelligence is accelerating the digital government journey. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/governing-with-artificial-intelligence_398fa287/795de142-en.pdf

OECD. (2019). The Path to Becoming a Data-Driven Public Sector. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/the-path-to-becoming-a-data-driven-public-sector_9ed7e867/059814a7-en.pdf

Scognamiglio, F., Ramachandran, S., Engelhardt, M., Santhanam, P., Gupta, A., Sherawat, P., Quinones, JR, Dunbar, A., Abdelrahman, B., and Øllgaard, D. BCG. Cloud Cover: Price Swings, Sovereignty Demands, and Wasted Resources. https://www.bcg.com/publications/2025/cloud-cover-price-sovereignty-demands-waste

Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M. and Lundgren, M. (2023). *The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research.*

UN DESA. E-Government Survey 2022: The Future of Digital Government. https://digitallibrary.un.org/record/3990059?v=pdf

Woersdoerfer, M. (2023). *AI Ethics and Ordoliberalism 2.0: Towards a Digital Bill of Rights.*

Yeung, K. (2018). Algorithmic Regulation: A Critical Interrogation. https://www.researchgate.net/publication/318820255_Algorithmic_regulation_A_critical_interrogation

Zuboff, S. (2019). *The Age of Surveilance Capitalism.*