

DOI: 10.47743/ejpar.2026-7-6

POLICIES FOR IMPROVING DIGITAL GOVERNANCE, SECURITY AND INDEPENDENCE IN GREECE

EFSTATHIA IOANNOU

National Centre for Social Research (EKKE)

Athens, Greece

ioannou@ekke.gr

THEODORE TSEKERIS

Centre of Planning and Economic Research (KEPE)

Athens, Greece

tsek@kepe.gr

Abstract

Despite Greece's important progress in digital governance significant challenges remain in the fields of digital governance, cybersecurity, and digital sovereignty. Institutional adaptation often lags behind technological change, while digital transformation progresses more slowly at peripheral areas. Public administration still suffers from fragmented procedures, incompatible data formats, and limited interoperability. In addition, Greece is currently considered a "beginner" in the EU's open data maturity rankings, as public sector data are not always accessible, machine-readable, or openly licensed. At the same time, the growing influence of multinational Big Tech companies raises concerns regarding state data sovereignty and dependency on external digital infrastructures. Public distrust related to privacy violations, the absence of regulatory and ethical frameworks for Artificial Intelligence, and fears of algorithmic bias further complicate the digital transition. Limited citizen participation in the design of automated decision-making systems, insufficient cybersecurity legislation, weak digital literacy, and the low adoption of open-source technologies also undermine resilience and transparency. The proposed solutions emphasise an integrated institutional, technological, and organisational strategy. Key measures include adopting a "digital by default" legislative approach and implementing the concept of "Law as Code." Stronger European and international cooperation is recommended to regulate digital monopolies and enhance digital independence through investments in infrastructure, software, Artificial Intelligence, and data governance. Further priorities include expanding open-data policies, strengthening interoperability, improving cybersecurity standards and personal data protection, enhancing public sector training, and promoting participatory governance through co-design processes involving citizens, experts, and businesses.

Keywords: digital governance; artificial intelligence; data policy; security; technological sovereignty.

JEL Classification: O33; O38; F52; L17; L86.

1. INTRODUCTION

Greece stands at a pivotal point in its digital transition, the successful outcome of which requires a holistic approach. Despite the progress achieved in recent years, the country continues to face a series of structural issues, such as low levels of government effectiveness, low regulatory quality, and lack of productive investment (KEPE, 2025). These issues undermine the effectiveness of digital governance, jeopardise data security, and severely limit the country's technological independence. Understanding these issues is a prerequisite for any meaningful intervention and the evaluation of relevant policies.

Despite the challenges, the current circumstances offer significant opportunities for digital acceleration and qualitative improvement, most notably through the financial support of the Greek Recovery and Resilience Plan (RRP) (Ladi, Tsarouhas and Copeland, 2025). Specifically, the RRP allocates approximately 23% of its budget towards the digital transition, creating a window of opportunity for systematic investment (European Commission, 2024). Provided that these resources are not utilised in a piecemeal manner (e.g., for purchasing technology), but to achieve specific digitisation milestones within the framework of a National Digital Transformation Plan, this will serve as a powerful incentive for administrative reform.

In the context of these challenges and prospects, this article first presents the current situation and problems associated with the digital governance, digital security and digital sovereignty in Greece (Section 2). Next, several opportunities to be exploited and prospects to reinforce digital governance are discussed (Section 3). Section 4 presents a comprehensive set of policy options, which can potentially foster democratic digital governance, digital security and transparency, and the national digital independence. Section 5 summarises and concludes with some policy recommendations.

2. CURRENT SITUATION AND CHALLENGES

One of the most fundamental problems observed in the digital transformation of public administration is the significant time lag in institutional adaptation relative to rapid technological advancements. A characteristic example is the absence of ethical frameworks for the use of Artificial Intelligence (AI) in the public sector, resulting in an increased risk of inconsistent implementation, lack of transparency and reduced accountability. This lack of transparency is accompanied by inadequate or ex-post risk assessments during the implementation of digital solutions — a fact that leaves critical infrastructure exposed to cyberthreats, undermines digital security, and increases vulnerability, highlighting gaps in prevention and operational readiness. The lack of a relevant security framework and systematic training for specialised personnel, limited resources, and the absence of a related culture within the public sector also contribute to this situation (Demertzis *et al.*, 2025).

At the same time, the use of AI systems based on historical data carries the risk of algorithmic bias, which can reproduce or even intensify social inequalities and exclusions, particularly in sensitive fields such as legal or administrative decisions. Addressing such phenomena becomes even more challenging, as AI regulation cannot be effectively managed at a national level but requires international cooperation (Deligiannis *et al.*, 2025). The cross-border nature of these technologies, largely offered by the foreign providers and global-scale platforms, and the speed of innovation diffusion pose the risk to the country finding itself in a position of technological—and beyond—dependency, limiting its sovereignty over data, critical digital infrastructure, and privacy protection.

The fragmentation of procedures, data formats, and information systems within public administration remains a primary obstacle. Many agencies operate in isolation – within 'silos' – with different and often incompatible technological infrastructures, resulting in limited interoperability and delays. In the data domain, serious deficiencies persist; although data are collected and made available through the National Open Data Portal, most of it remains inaccessible, lacks open licensing, documentation access and communication mechanisms with its administrators. Furthermore, the percentage of data available in machine-readable format is extremely low (European Commission, 2025). Additionally, there are no mechanisms for publishing dynamic data in real-time, nor are there sufficient procedures for monitoring the impact and reuse of data across different agencies.

Bureaucracy is often simply digitalised instead of being simplified before going digital. Furthermore, the lack of interoperability between agencies hinders the easy and secure exchange of information, while the exclusion of citizens from the design of automated decision-making systems leads to a deficit in democratic legitimacy. Ultimately, the digital transformation risks becoming a tool of exclusion if it does not take into account the digital divide caused by low educational and income levels in certain regions, or even by unequal internet access. Rather than mitigating these disparities, technology may exacerbate them, creating new forms of digital social and territorial exclusion.

3. OPPORTUNITIES AND PROSPECTS

Effective digital governance can help to achieve increased citizen participation in decision-making, simplify processes, and modernise services. Moreover, effective digital governance enhances transparency, accountability, meritocracy, democracy, economic growth, and social inclusion. Although the integration of AI in the Greek public sector is still in its early stages, it bears great potential (Mantas, Karapetsas and Malik, 2025), through placing citizens at the core of services delivered, providing faster access to public documents and upgraded connectivity (digital issuance of certificates, licenses, and permits; electronic case processing; debt payments etc.). The country's highly skilled IT workforce can contribute decisively to this direction so as to reverse the brain

drain. The success of open government and administrative oversight initiatives, such as the 'DIAVGEIA' portal, demonstrates the positive impact of open data on decision-making and the strengthening of citizen trust when such measures are strictly adhered to (Kapantai, Mitropoulou and Deligiannis, 2025).

The European Union has placed technological sovereignty and autonomy at the top of its agenda, including policy initiatives such as the EU Strategic Autonomy plan, the European Chips Act and the European Critical Raw Materials Act (European Parliament, 2022; European Union, 2023; European Commission, 2023). Leveraging the European regulatory framework, such as the Data Act and the Data Governance Act, shifting towards open-source software, and protecting data as public goods, strengthen interoperability and data sovereignty, aiming to achieve digital independence and counter the dominance of big-tech companies. Cutting-edge technologies, such as blockchain, IoT, and big data analytics, act as accelerators for improved planning and policy-making, while increasing transparency, inclusiveness, and the efficiency of public administration. At the same time, AI can automate time-consuming administrative processes and extract valuable insights from public sector data, contributing to the development of targeted policies and legislation. Furthermore, the advancement of digital platforms allows for broader participation in decision-making through collaborative tools and virtual meetings. The establishment of Communities of Practice (CoPs) and the adoption of models of co-creation, co-production, and co-evaluation of policies with citizen participation strengthen innovation and the democratic design of digital policies.

At the international level, Greece's participation in initiatives such as the Open Government Partnership (OGP) contributes to the improvement of legislation and digital governance. The development of 'AI Giga-Factories' within the EU framework offers a significant opportunity for Greece to act as an accelerator for startups and to spread AI capabilities throughout the domestic business ecosystem. Finally, strengthening the cooperation between public and private sectors can provide further boost for the implementation of innovative digital projects.

4. PROPOSED POLICY OPTIONS

4.1. Policies for Democratic Digital Governance

The transition towards secure and socially just digital governance requires a coherent framework of change that extends beyond technological shifts, necessitating coordination between ethical principles, technical requirements, and legal compliance (Stasinopoulos, 2025). This framework comprises three pillars: institutional modernisation, technological upgrading, and strengthening of human capital to empower governance, safeguard security, and foster independence. It is essential to develop transparent and inclusive digital governance that incorporates local and regional strategies to address real needs, while, at the same time,

providing incentives for small and medium-sized enterprises to adopt new technologies that will act as a lever for productivity and competitiveness.

Democratic procedures must reside at the core of policy design, avoiding horizontal planning and prioritizing public consultation through existing platforms, such as OpenGov. Furthermore, the focus must remain on the social dimension and the human factor, ensuring that technology is integrated into policies that reduce inequalities and expand rights, rather than transposing existing exclusions into the digital environment (Demertzis *et al.*, 2025). To this end, for instance, access to high-speed digital connectivity should be universal, even in remote areas.

The organisation of co-creation and co-evaluation workshops on relevant public policies is proposed, involving diverse population groups from the design phase so as to ensure that digital policies are inclusive and gain broader social acceptance. This can be achieved within the framework of CoPs—collaborative networks acting as 'idea incubators'—facilitating cooperation between competent bodies, transforming scattered knowledge into applicable, fair digital policies, and formulating evidence-based policy proposals for the State (Deligiannis *et al.*, 2025). Within the public sector, the formation of multidisciplinary policy-design teams is recommended, focusing on the user and aligning with current digital policies. Regarding policymaking and legislation, it is essential to integrate the digital dimension so that new legislation is digitally compatible and 'digitally ready' by design. For this purpose, the 'Law as Code' approach may be utilised where appropriate, guided by the 'digital by design' principle (Spiliopoulou, Mitropoulou and Deligiannis, 2025).

The use of emerging technologies, such as the Internet of Things (IoT) and AI, by public administration is recommended to focus on critical sectors such as the environment, transportation, health, education, and civil protection. Their regulation is imperative to ensure the protection of privacy and the avoidance of discrimination and inequalities, as well as to mitigate the risks of disinformation, manipulation, the undermining of democratic processes, data breaches, and decision-making without the possibility of human intervention. Specifically regarding AI, a comprehensive set of measures is required, such as specialised trainers, the enhancement of digital literacy, lifelong learning, transparency in its use, and the validation of its outputs.

4.2. Policies for Digital Security and Transparency

At the heart of these reforms must be a coherent data policy that ensures quality, security, and ease of access through the national portal, while encouraging the development of digital services. The implementation of interoperability standards will eliminate 'silos' and facilitate the smooth exchange of data and the compatibility between agency systems. Furthermore, the adoption of the 'Once-Only' principle will allow citizens to submit information just once, enabling the state to circulate these data internally with security and respect for personal data

(General Data Protection Regulation-GDPR). The adoption of the European Data Catalogue vocabulary Application Profile (DCAT-AP) standard and the creation of a metadata guide are essential steps towards system interoperability, the upgrading of public services, and the reduction of bureaucracy.

The publication of data by public bodies should be made mandatory, accompanied by clear timelines. Public entities holding high-value datasets must implement the relevant regulation, while it is imperative that all government acts and decisions be posted on the DIAVGEIA portal to be legally binding, fostering transparency and public oversight. The protection of personal data must be ensured through Data Protection Impact Assessments (DPIAs), in accordance with GDPR requirements, so that risks are prevented rather than addressed ex-post.

The utilisation of big data should be conducted with careful attention to representativeness, in order to mitigate bias during the training of AI models and to optimise policy decisions. The development of Open API applications and the use of cloud technologies with open interconnection protocols will facilitate the secure exchange of information between agencies. At the same time, the upgrading of unified digital registries will contribute to data transparency and reliability, simplification of procedures, and improved coordination across the public sector.

Training public servants on open data, metadata, and the culture of openness and security is deemed imperative. Adherence to the FAIR (Findability, Accessibility, Interoperability, Reusability) principles and the principles of Open Government Data, such as machine readability, timely availability, licensing, and ease of access constitutes the guarantee for a digital transformation that serves the public interest.

4.3. Policies for National Digital Independence

In addition, a multi-level approach that combines national policies with international cooperation to regulate the concentration of power among multinational digital technology corporations—using European and international tools and creating open and accessible digital infrastructures—will contribute to achieving digital independence. This independence must extend from software and data to data centers, infrastructure, and energy, thereby protecting the country from the 'techno-feudalism' of major multinationals, and preventing political decision-making from being influenced by digital oligopolistic lobbies (Papaevangelou and Siapera, 2025). Public-private partnerships can play a key role in reaching this goal.

Security and resilience are the core pillars of these changes, serving as a horizontal priority that permeates all the aforementioned actions. The integrity of documents can be ensured through the implementation of blockchain technology, while protection against threats can be strengthened by unified security standards. Cybersecurity policies must be robust, given the management of large data volumes and increased digitisation. They should not be addressed in a fragmented manner, but as an inviolable prerequisite for every digital application, with risk

assessment provisions at all stages—from the design phase to the conduct of regular audits and with immediate response to serious incidents. In conclusion, through this holistic and participatory approach, Greece can build a digital future that will be at the same time advanced, secure and democratic.

5. CONCLUSIONS

Effective and secure digital governance is a critical pillar for strengthening technological independence and resilience. Despite Greece's positive strides in digital governance, through platforms such as gov.gr and the Mitos registry, multiple challenges have been identified in the field of digital governance and cybersecurity, related to both the institutional maturity and the operational readiness of state mechanisms. The identified problems—institutional gaps, fragmented security mechanisms, dependence on external technology providers, and limited adoption of open technologies—point to the need for far-reaching reforms that will strengthen the country's operational security and digital sovereignty.

The proposed solutions form a multi-level framework for action at the institutional, technological, and organisational levels, focusing on strengthening cybersecurity, adopting open-source technologies, the education of citizens and public officials, and the safeguarding of digital independence. Through these measures, the country can achieve a more mature, secure, and democratically grounded digital governance system, capable of responding to the challenges of the new digital era. Moreover, targeted policy interventions to foster technological specialisation and innovation can strengthen Greece's role in the global semiconductor ecosystem (Karampekios *et al.*, 2026).

Synergies between economic, social, and digital policy and the adoption of a comprehensive (co-design) approach to legislation are required, so that every law is accompanied by an internationally defined (EU, UN, OECD) digital strategy to regulate the centralisation of multinational digital technology companies. Furthermore, the development of a data policy to encourage the growth of digital services and the implementation of a robust digital security policy should be a prerequisite for all digital applications. Last, the protection of personal data as well as data interoperability should be ensured through impact assessment procedures.

ACKNOWLEDGEMENTS

This article is partly based on the outcome of the JustReDI (Resilience, Inclusiveness and Development: Towards a Just Green and Digital Transition of Greek Regions) project – TAEDR-0537352, which was realised in the course of the National Recovery and Resilience Plan 'Greece 2.0' with the funding of the European Union – NextGenerationEU, Athens: EKKE-AthenaRC-NOA-HCMR-IHU-UNIWA. Sincere acknowledgements are expressed to the participants and authors of the JustReDI project deliverables: N. Alonistioti, G. Bithymitris, D. Charitos, A. Deligiannis, Ch. Deligiannis, N. Demertzis, D. Gouskos, E. Kapantai, N. Klironomos, K. Mandenaki, A. Melidis, D. Mitropoulou, B. Peristeras, N. Stasinopoulos, Ch. Tsekeris, Th. Tsekos.

References

- 1) Deligiannis, A., Mitropoulou, D., Melidis, A. and Spiliopoulou, P. (2025). Digitally compatible law-making and policy-making. In: Demertzis, N. and Papadoudis, G., eds., *Resilience, Inclusion and Growth: A Triptych for the Twin Transition of Greek Regions*, Athens, Greece: EKKE, Papazisis Publishers, pp. 63-78.
- 2) Demertzis, N., Tsiganou, I., Avrami, L., Artelaris, P., Tsekeris, C., Stasinopoulos, N., Kondyli, D., Kaminariaris, O. and Papadoudis, G. (2025). Pioneers and laggards in the green and digital transition: implementation challenges for the Greek regions. In: Demertzis, N. and Papadoudis, G., eds., *Resilience, Inclusion and Growth: A Triptych for the Twin Transition of Greek Regions*, Athens, Greece: EKKE, Papazisis Publishers, pp. 45-61.
- 3) European Commission (2023). *European Critical Raw Materials Act*. Brussels, Belgium: European Commission. [online] Available at: https://commission.europa.eu/document/download/20fd33a4-e426-403c-afc1-c523d5d3e7c7_en [Accessed 28.05.2026].
- 4) European Commission (2024). *Greece 2024 Digital Decade Country Report*. Brussels, Belgium: European Commission. [online] Available at: <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports> [Accessed 28.05.2026].
- 5) European Commission (2025). *DESI Dashboard for the Digital Decade*. Brussels, Belgium: European Commission. [online] Available at: <https://digital-decade-desi.digital-strategy.ec.europa.eu/> [Accessed 28.05.2026].
- 6) European Parliament (2022). *EU Strategic Autonomy 2013-2023 - From Concept to Capacity*. European Parliament Briefing, July 2022. [online] Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI\(2022\)733589_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf) [Accessed 28.05.2026].
- 7) European Union (2023). *Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act)*. Brussels, Belgium: The European Parliament and the Council of the European Union. [online] Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1781> [Accessed 28.05.2026].
- 8) Kapantai, E., Mitropoulou, D. and Deligiannis, A. (2025). Openness and participation. In: Demertzis, N. and Papadoudis, G., eds., *Green, Digital and Twin Transition in Greece: Short Essays on Great Challenges*, Athens, Greece: EKKE, Papazisis Publishers, pp. 215-222.
- 9) Karampekios, N., Sioumalas-Christodoulou, K., Angelakis, A. and Carayannis, E.G. (2026). A research agenda for the Greek semiconductors sector ecosystem: Enabling the transition from emerging capabilities to strategic integration. *Journal of the Knowledge Economy*. [online] Available at: <https://doi.org/10.1007/s13132-026-03305-y> [Accessed 28.05.2026].
- 10) KEPE (2025). *Greek National Productivity Board Annual Report 2025: Development through Institutional and Industrial Reforms*. Athens, Greece: Centre of Planning and Economic Research. [online] Available at: <https://www.kepe.gr/prosfates->

- dimosieyseis/ethniko-symvoulío-paragwigikotias/ethsies-ekthesis/ethniko-symvoulío-paragwigikotitas-etisia-ekthesi-2025/ [Accessed 28.05.2026].
- 11) Ladi, S., Tsarouhas, D. and Copeland, P. (2025). Negotiating the recovery and resilience facility: the emergence of coordinative conditionality. *Comparative European Politics*, 23(1), pp. 18-39. [online] Available at: <https://link.springer.com/article/10.1057/s41295-024-00385-5> [Accessed 28.05.2026].
 - 12) Mantas, C., Karapetsas, V. and Malik, S. (2025). The usage of AI in the public sector: The case of Greece and proposals for future research. In: M.D. Lytras and A.C. Şerban, eds., *Education, Future Jobs and Smart Systems in the Age of Artificial Intelligence, Part A: AI Transformations in Education and Workforce Development*. Leeds, UK: Emerald, pp. 111-127.
 - 13) Papaevangelou, C. and Siapera, E. (2025). State, platform capitalism and infrastructural power: Microsoft's data centres in Greece 2.0. *Platforms & Society*, 2. [online] Available at: <https://doi.org/10.1177/29768624251323325> [Accessed 28.05.2026].
 - 14) Spiliopoulou, P., Mitropoulou, D. and Deligiannis, A. (2025). Digitally ready legislation – essential for a fair green and digital transition. In: Demertzis, N. and Papadoudis, G., eds., *Green, Digital and Twin Transition in Greece: Short Essays on Great Challenges*, Athens, Greece: EKKE, Papazisis Publishers, pp. 209-214.
 - 15) Stasinopoulos, N. (2025). Digital transformation in the context of social and economic development. In: Demertzis, N. and Papadoudis, G., eds., *Green, Digital and Twin Transition in Greece: Short Essays on Great Challenges*, Athens, Greece: EKKE, Papazisis Publishers, pp. 157-162.