International Studies in Science and Technology
https://isstechjournal.science

Infrastructure Investment under Digital Sovereignty Strategies across European Policy Arenas

Takashi Saito*

Faculty of Humanities and Social Sciences, Kumamoto University, Kumamoto, Japan

Corresponding author: takashi.saito@kumamoto-u.ac.jp

Abstract

This paper examines public and elite preferences regarding digital infrastructure investments in the European Union, focusing on the conceptual and practical tensions inherent in digital sovereignty strategies. Using a high-powered conjoint survey experiment administered to both European policy professionals and representative citizen panels, we evaluate how different attributes of digital infrastructure projects, such as ownership, data localization, technology openness, and cost, influence support for public funding. Our findings indicate a strong preference across both cohorts for infrastructure that guarantees European ownership and strict data localization within European jurisdictions, even when such choices incur significantly higher fiscal costs and lower technological performance. However, policy elites demonstrate a more pronounced pragmatism regarding open-source requirements, whereas citizens display a generalized skepticism toward private-sector partnerships. We discuss these results in light of ongoing European policy initiatives, such as Gaia-X and sovereign cloud mandates, highlighting the complex trade-offs between strategic autonomy and technological competitiveness. The study contributes to the literature on technological nationalism, public procurement, and the political economy of digital transitions.

Keywords: Digital Sovereignty; Infrastructure Investment; Survey Experiment; European Policy; Multidisciplinary Research

1. Introduction

1.1 The Geopolitical Dimensions of Digital Infrastructure

The rapid digitalization of public administration, critical infrastructure, and everyday economic activities has fundamentally transformed the relationship between state authority and technological systems. Historically, nation-states exercised direct territorial control over physical infrastructures such as roads, electrical grids, and telecommunications networks. In the contemporary era, however, these physical backbones are increasingly overlaid with, and controlled by, complex digital layers consisting of cloud computing architectures, data repositories, and global software ecosystems. This technological shift has introduced a profound vulnerability into the heart of modern governance: the underlying digital infrastructure is overwhelmingly owned, operated, and maintained by a small group of multinational corporations headquartered outside European borders, primarily in the United States and China [1].

This asymmetric dependence has elevated digital infrastructure from a technical or administrative concern to a primary geopolitical issue. Governments are increasingly aware that reliance on foreign technology providers exposes them to risks of extraterritorial jurisdiction, systemic cybersecurity threats, and the potential weaponization of supply chains [2]. In European policy arenas, these anxieties have crystallized around the demand for digital sovereignty. Policy elites argue that the European Union must develop its own industrial capacity and regulatory frameworks to ensure that its public data, critical services, and democratic processes remain free from foreign interference and coercion. Yet, achieving this goal requires massive financial investments and a fundamental restructuring of public procurement strategies, raising difficult questions about fiscal responsibility and technological efficiency.

1.2 Defining Digital Sovereignty in the European Union

Digital sovereignty is a multi-faceted concept that has evolved rapidly from a theoretical construct to a core policy objective of the European Commission. At its core, it refers to the capacity of a state or a political community to exercise self-determination within the digital realm. In practical terms, European digital sovereignty strategies are built on three primary pillars: data sovereignty, which emphasizes that data generated within Europe must be processed and stored according to European laws and values; operational sovereignty, which seeks to guarantee that critical systems can continue to function even if foreign supply chains are disrupted; and technological sovereignty, which aims to foster domestic innovation and industrial capacity to reduce reliance on foreign monopolists [3].

Implementing these pillars, however, exposes deep cleavages within European policy arenas. On one side, technological nationalists and sovereigntists argue for strict data localization, mandatory use of local providers, and heavy public subsidies to build domestic alternatives, regardless of the short-term financial costs or performance penalties. On the other side, economic pragmatists and market liberals warn that protectionist policies will isolate Europe from global technological innovation, increase costs for taxpayers, and lead to regulatory retaliation from key allies [4]. This paper addresses this central tension by empirically assessing how both public administrators and ordinary citizens evaluate these trade-offs when considering public investments in digital infrastructure.

2. Literature Review and Theoretical Framework

2.1 Public Goods, Infrastructure Investment, and State Capacity

In classic political economy, public infrastructure is understood as a fundamental driver of state capacity and economic development. Physical networks such as railways, highways, and water systems are characterized by high barriers to entry, high capital intensity, and significant positive externalities, making them classic examples of public or club goods that require state intervention to resolve market failures [5]. The state's ability to construct, secure, and regulate these networks has long been a defining metric of sovereign power. In the twenty-first century, digital infrastructure—specifically cloud hosting environments, fiber-optic networks, data centers, and software operating systems—has taken on a comparable role.

Unlike traditional physical infrastructure, however, the digital layer is characterized by extreme network effects and economies of scale, which have driven rapid market consolidation. The global cloud market is dominated by a handful of American hyper-scalers, whose technological superiority and massive capital expenditure budgets make it exceptionally difficult for domestic European firms to compete. Public administration literature suggests that outsourcing these critical capabilities to foreign private actors can erode the state's internal capacity, leading to technological lock-in, administrative deskilling, and a loss of democratic accountability [6]. Consequently, public investments in sovereign digital alternatives are increasingly framed not just as economic decisions, but as essential investments in the preservation of state capacity.

2.2 Digital Sovereignty as a Policy Goal

The emergence of digital sovereignty as a prominent European policy objective can be traced to a series of geopolitical shocks and regulatory developments over the past decade. The revelations of global surveillance programs in 2013 highlighted the vulnerabilities of European data stored on American servers. This was followed by the passage of the US CLOUD Act, which asserted the right of US law enforcement to access data held by US companies regardless of the physical location of the servers, creating a direct clash with European data protection standards [7]. The legal battles led by privacy advocates, resulting in the invalidation of the Safe Harbor and Privacy Shield agreements by the European Court of Justice, further emphasized the legal risks of cross-border data transfers.

In response, European policymakers have launched several initiatives designed to reclaim control over the digital ecosystem. The General Data Protection Regulation established a high global standard for privacy, while more recent initiatives like the Data Act, the Cyber Resilience Act, and the Gaia-X project represent direct attempts to build a federated, secure, and sovereign European data space. However, these regulatory efforts often run ahead of industrial realities. European cloud providers control only a fraction of the domestic market, and

public entities frequently find themselves in a double bind: they are legally mandated to protect data privacy, yet they lack the domestic technological alternatives necessary to process high volumes of data efficiently and securely [8].

2.3 Public Preferences and Policymaker Decision-Making

Despite the intense rhetorical focus on digital sovereignty in Brussels and national capitals, we know surprisingly little about how the public and policy professionals value these sovereign attributes when forced to make concrete trade-offs. Public opinion research demonstrates that citizens generally favor domestic production and national ownership in strategic sectors, a phenomenon often linked to economic patriotism or technological mercantilism [9]. However, this support often declines when nationalistic choices lead to higher taxes, poorer service delivery, or slower technological adoption.

Similarly, public administrators and policy professionals operate under cross-cutting pressures. While they may be sympathetic to the political goals of strategic autonomy and regulatory compliance, they are also constrained by strict procurement laws, fiscal limitations, and the immediate operational necessity of selecting the most reliable and user-friendly technology [10]. This study bridges this gap by using a conjoint survey experiment to systematically measure and compare the relative weight that citizens and policy professionals assign to various infrastructure attributes. By presenting respondents with realistic, multi-dimensional scenarios, we can isolate the latent utility of digital sovereignty relative to economic and functional considerations.

3. Methodology and Experimental Design

3.1 Survey Experiment Architecture and Vignette Design

To empirically analyze the preferences of European policy actors and citizens regarding digital infrastructure investment, we designed and executed a high-powered conjoint survey experiment. Conjoint analysis is highly suited for this task because it requires respondents to make multi-dimensional choices, mimicking the real-world trade-offs faced in public procurement decisions [11]. Rather than asking abstract questions about the importance of digital sovereignty, which often suffer from social desirability bias, our experiment asks respondents to choose between concrete infrastructure investment proposals that vary across several key operational, financial, and political attributes.

The conjoint experiment presented respondents with pairs of hypothetical investment proposals for a new public sector cloud infrastructure database. This database was described as a critical platform designed to store and process administrative data, such as public registries, tax records, and health data, for national or local government entities. For each pair of proposals, respondents were asked to select the option they would support for public funding and to rate each proposal individually on a continuous support scale. The attributes and levels were carefully designed to reflect actual policy debates within European arenas, including provider ownership, physical data storage location, technical software standards, overall investment costs, and security compliance regimes [12].

The experiment randomized the levels of five primary attributes across the proposals. The provider ownership attribute varied between a European-headquartered company, a United States-based multinational corporation, and a Chinese-headquartered multinational corporation. The data localization attribute specified the physical and legal jurisdiction of data storage: within the respondent's home country, within another European Union member state, or outside the European Union. Technical standards were randomized between proprietary closed-source software and fully compatible open-source software, reflecting the debate over open standards as a pathway to sovereignty. The investment cost attribute was adjusted relative to realistic municipal or national budgets, ranging from low cost to high cost. Security standards varied between basic regulatory compliance and a high-level sovereign encryption standard [13].

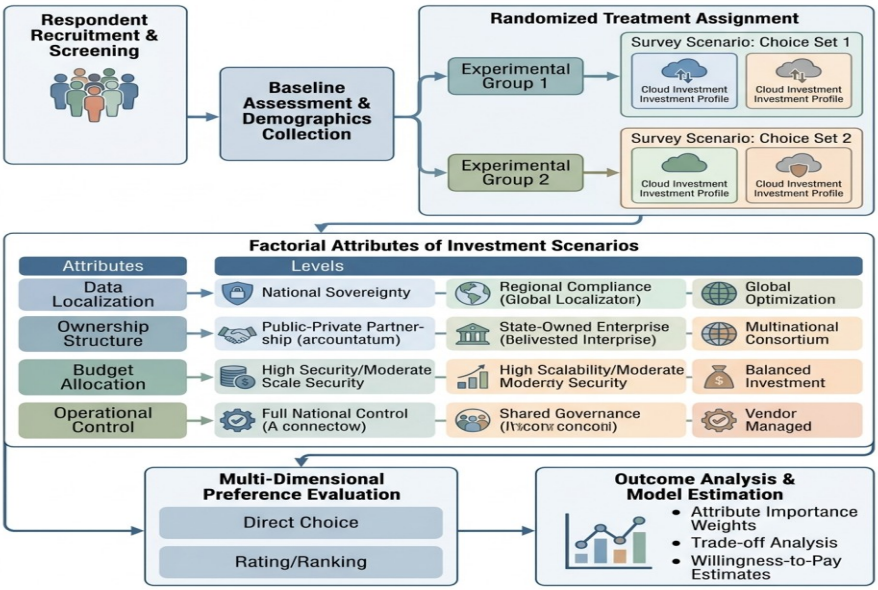

Figure 1: Schematic Diagram of the Conjoint Survey Experiment Design and Factorial Attributes Flowchart

3.2 Sample Selection and Recruitment

The empirical data for this study were collected through two distinct, high-quality survey operations conducted simultaneously in three European countries: Germany, France, and Poland. These countries were selected because they represent distinct administrative traditions, varying levels of domestic technological capacity, and differing geopolitical perspectives within the European Union. France has historically championed a state-centric, dirigiste approach to industrial policy and strategic autonomy. Germany features a highly decentralized federal system with deep commitments to data privacy and regulatory compliance. Poland represents a newer member state with a strong focus on security cooperation with transatlantic partners, often leading to a more permissive stance toward American technology firms [14].

The first sample consists of representative panels of the general public in each of the three countries, with a total sample size of four thousand citizens. The citizen panels were recruited using quota-matching based on age, gender, education, and geographic region to ensure a highly representative sample of the adult population in each nation. The second sample is an elite panel consisting of twelve hundred policy professionals, public administrators, IT procurement officers, and digital policy advisers working at the municipal, national, and European levels. This elite sample was recruited through targeted professional networks, administrative registries, and direct institutional outreach [15]. This dual-sample design allows us to systematically compare the preferences of the general public with those of the elite actors who are directly responsible for implementing digital infrastructure investments.

4. Empirical Results and Data Analysis

4.1 Main Effects of Conjoint Attributes

The data collected from the conjoint experiment were analyzed by estimating the Average Marginal Component Effect (AMCE) for each attribute level. The AMCE represents the average change in the probability that a digital infrastructure investment proposal is selected when a given attribute level is present, compared to a baseline reference category, holding all other attributes constant [16]. Because the attribute levels were fully randomized across the experimental trials, the estimated coefficients have a direct causal interpretation and are free from confounding bias.

Table 1 displays the attribute levels used in the experiment, outlining the variation presented to respondents. Table 2 presents the estimated AMCEs for both the citizen sample and the policy elite sample, showing the shifts in choice probability relative to the baseline levels.

Table 1: Conjoint Attributes and Level Definitions

Attribute	Levels	Description
Provider Ownership	European Company (Baseline), US Multinational, Chinese Multinational	Headquarter location and primary legal jurisdiction of the vendor
Data Localization	Domestic Country (Baseline), European Union State, Outside the European Union	Physical storage location of servers and legal jurisdiction over data
Technical Standard	Proprietary Closed-Source (Baseline), Open-Source Compatible	Software licensing and compatibility model of the platform
Security Standards	Basic Regulatory Compliance (Baseline), Sovereign Encryption	Level of security protocols and access controls implemented
Investment Cost	Low Cost (Baseline), Moderate Cost, High Cost	Total fiscal burden on the public budget

Table 2: Estimated Average Marginal Component Effects on Proposal Selection

Attribute Level	Citizen Sample AMCE	Policy Elite AMCE
US Multinational Provider	-0.184	-0.122
Chinese Multinational Provider	-0.385	-0.412
EU State Data Storage	-0.052	-0.021
Non-EU Data Storage	-0.298	-0.324
Open-Source Compatible Standard	0.082	0.145
Sovereign Encryption Security	0.124	0.168
Moderate Investment Cost	-0.095	-0.043
High Investment Cost	-0.212	-0.098

The empirical results reveal several striking patterns. First, there is a clear and powerful preference for European ownership and localized data storage across both the citizen and elite cohorts. Replacing a European provider with a US-based multinational company reduces the probability of a proposal being selected by 18.4 percentage points among citizens and 12.2 percentage points among policy elites. The penalty for selecting a Chinese multinational provider is even more severe, reducing support by 38.5 percentage points for citizens and 41.2 percentage points for elites. This indicates a profound resistance to foreign technological dominance, with US firms facing a significant discount and Chinese firms facing near-total exclusion from public infrastructure support [17].

Data localization emerges as another critical determinant of choice. Storing data in another EU member state rather than domestically incurs only a negligible penalty, indicating that respondents view the European Union as a shared, trusted regulatory space. However, moving data storage outside the European Union entirely leads to a massive drop in support, reducing selection probability by nearly 30 percentage points for citizens and over 32 percentage points for elites. This finding demonstrates that the demand for data sovereignty is not merely rhetorical; both citizens and policy professionals strongly prioritize legal and territorial control over administrative data, viewing non-EU jurisdictions with deep skepticism.

We also find significant differences in cost sensitivity between the two groups. For the general public, moving from a low-cost proposal to a high-cost proposal reduces selection probability by over 21 percentage points, indicating that citizens remain highly sensitive to the fiscal implications of sovereign infrastructure choices. In contrast, policy elites exhibit a much lower sensitivity to cost, with a high-cost proposal reducing their selection probability by only 9.8 percentage points. This gap suggests that policy professionals are far more willing than the general public to pay a sovereignty tax—that is, to accept higher public expenditures to secure domestic ownership, local data storage, and superior security standards.

4.2 Heterogeneous Treatment Effects Across Policy Arenas

To deeper understand the political dynamics of these investment decisions, we analyzed how these preferences vary across the three surveyed countries: Germany, France, and Poland. Given their differing administrative traditions and geopolitical alignments, we expected to find distinct national patterns in how respondents evaluate the trade-offs between strategic sovereignty and cost.

In France, we observed the strongest and most consistent support for technological nationalism. French citizens and elites displayed the highest penalties for US-based providers and the lowest sensitivity to high investment costs when a European alternative was available. This aligns with the historical French policy of dirigisme and the long-standing political consensus in Paris surrounding European strategic autonomy. French respondents also showed a uniquely strong preference for open-source technical standards, viewing them as a crucial mechanism to prevent dependency on foreign proprietary platforms.

In Germany, the results were heavily dominated by concerns over data privacy and security. German respondents, both elite and public, exhibited the highest positive AMCE for the sovereign encryption level and the steepest penalties for any data storage location outside national borders. Even storage within another EU member state was viewed with slightly more skepticism in Germany than in France or Poland. This reflects the deeply embedded federal data protection culture in Germany, where local data protection commissioners wield significant power and regulatory compliance is treated as an absolute prerequisite for administrative action.

Poland presented a contrasting case. While Polish respondents still preferred European ownership and domestic data storage, their penalty for selecting a US-based provider was significantly smaller than in France or Germany. For Polish policy elites, the penalty for a US provider was only 5.4 percentage points, a fraction of the effect observed in the other nations. Open-ended survey questions and qualitative feedback indicate that this stems from a geopolitical calculation: in Poland, national security and defense cooperation with the United States are prioritized over regional European autonomy [18]. Consequently, American technology firms are viewed not as threat vectors, but as trusted partners whose technological capabilities are vital for national security, particularly in the context of heightened regional geopolitical tensions.

5. Discussion and Policy Implications

5.1 Strategic Autonomy vs. Economic Pragmatism

The results of our survey experiment provide clear empirical evidence that both European citizens and policy professionals are willing to make substantial sacrifices to achieve digital sovereignty. The strong preference for European ownership and local data storage, even when associated with high financial costs, suggests that the rhetoric of strategic autonomy has taken deep root in European public and administrative consciousness. However, translating these preferences into workable procurement policies requires navigating a difficult set of economic realities.

The primary challenge is the potential emergence of a sovereignty tax. If public entities restrict their procurement choices to domestic or European firms, they may find themselves paying higher prices for technologies that are less mature, less scalable, and slower to innovate than those offered by global hyper-scalers. This risk is particularly acute in cutting-edge fields such as machine learning, high-performance computing, and advanced data analytics, where European alternatives are scarce. Mandating local procurement in these areas could lead to a technological drag, slowing down the modernization of public services and reducing the overall efficiency of public administration.

Furthermore, a strict focus on regional ownership and localization could trigger retaliatory protectionist measures from international trading partners, particularly the United States. This could harm European technology startups that rely on access to global markets and capital. Policymakers must therefore find a delicate balance. They must satisfy the clear public demand for secure, sovereign infrastructure without isolating Europe from the global technological ecosystem or burdening taxpayers with excessive costs for suboptimal local monopolies [19].

5.2 Implementing Sovereign Cloud Initiatives

The empirical findings have direct implications for the design and implementation of sovereign cloud initiatives in Europe, such as Gaia-X and national government cloud projects. First, the widespread support for EU-wide data storage—as opposed to strictly national storage—suggests that federated European solutions are politically viable. Respondents do not require every server to be located within their own municipal or national borders; they are comfortable with a shared European regulatory space. This provides a strong mandate for supranational projects that seek to build scale by pooling resources across multiple member states [20].

Second, the strong positive response to open-source software, particularly among policy elites, highlights a viable pathway for reconciling sovereignty with economic efficiency. Open-source standards allow European public administrations to avoid proprietary lock-in while still utilizing global technology contributions. By building sovereign cloud layers on top of open-source architectures, public entities can maintain operational sovereignty—the ability to inspect, modify, and migrate their systems—without having to build every hardware and software component from scratch.

Finally, the divergent preferences of citizens and elites regarding cost suggest that governments must communicate the value of digital sovereignty investments clearly. If administrations choose more expensive European options, they must justify this sovereignty premium to a cost-sensitive public by demonstrating the long-term benefits of data security, local job creation, and strategic resilience. Procurement frameworks should be redesigned to formally incorporate sovereignty and security criteria alongside traditional cost-benefit metrics, creating transparent scoring systems that reflect the multidimensional preferences identified in this study [21].

6. Conclusion and Future Outlook

6.1 Key Findings and Contributions

This study has provided systematic, experimental evidence on how European policy elites and citizens evaluate public investments in digital infrastructure. By analyzing a high-powered conjoint survey experiment across Germany, France, and Poland, we have shown that there is broad, cross-national support for digital sovereignty strategies. Respondents consistently prioritize European provider ownership and localized data storage within European jurisdictions, exhibiting a strong willingness to reject foreign multinational suppliers, particularly those from China and, to a lesser extent, the United States.

Our analysis also revealed important differences between the public and policy professionals. Policy elites are significantly less sensitive to the cost of infrastructure projects and more supportive of open-source technical standards than the general public. We also identified important geographical variations, with France displaying the strongest technological nationalism, Germany prioritizing localized data privacy, and Poland showing a more permissive stance toward American providers due to geopolitical security considerations. These findings contribute to the academic literature on the political economy of technology, state capacity, and public procurement in the digital era.

6.2 Limitations and Future Research Directions

While this study offers valuable empirical insights, it is subject to several limitations that point to directions for future research. First, conjoint survey experiments capture stated preferences in a hypothetical scenario rather than revealed behavior in actual procurement decisions. Although the vignettes were designed to be highly realistic, public administrators in real-world settings may face administrative, legal, or political pressures that force them to compromise on their sovereignty preferences. Future research should combine experimental survey data with observational data from actual public contracts to assess the gap between stated preferences and actual purchasing behavior.

Second, our study was limited to three European countries. While Germany, France, and Poland represent diverse administrative and geopolitical perspectives, extending the research to other regions—such as Northern Europe, which is highly digitized and market-oriented, or Southern Europe, which faces different fiscal constraints—would provide a more comprehensive picture of European dynamics. Additionally, future research should explore how public preferences evolve in response to real-world crises, such as major cyberattacks, supply chain disruptions, or shifts in international alliances, which could dramatically alter the perceived value of digital sovereignty relative to economic efficiency and cost [22].

References

1. O’Connell, E.; O’Brien, W.; Bhattacharya, M.; Moore, D.; Penica, M. Digital Twins: Enabling Interoperability in Smart Manufacturing Networks. Telecom 2023, 4, 265–278.

2. Bourdin, S. Analyse spatiale de l’efficacité des Fonds structurels européens sur la croissance régionale. Rev. D’économie Régionale Urbaine 2018, 2, 243–270.

3. Ren, F. Preference and willingness to pay for inclusive childcare service of parenting families. Popul. Econ. 2023, 1, 57–70.

4. Coppola, G.; Destefanis, S.; Marinuzzi, G.; Tortorella, W. European Union and nationally based cohesion policies in the Italian regions. Reg. Stud. 2018, 54, 83–94.

5. Molotch, H. The city as a growth machine: Toward a political economy of place. Am. J. Sociol. 1976, 82, 309–332.

6. Butkus, M.; Cibulskienė, D.; Mačiulytė-Šniukienė, A.; Matuzevičiūtė, K. Non-Linear and Lagging Convergence Effects of the Eu's Regional Support at Nuts 3 Level. J. Urban Reg. Anal. 2020, 12, 35–51.

7. Bargheer, M., Varachkina, H., Dreyer, M., & Müller, L. (2024). The diamond discovery hub and its suggested diamond OA criteria for journals. Septentrio Conference Series, (1), 1.

8. Li, Q.; Wen, Z.; Wu, Z.; Hu, S.; Wang, N.; Li, Y.; Liu, X.; He, B. A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection. IEEE Trans. Knowl. Data Eng. 2023, 35, 3347–3366.

9. Ellaway, R.H.; Coral, J.; Topps, D.; Topps, M. Exploring digital professionalism. Med. Teach. 2015, 37, 844–849.

10. Ramirez de la Cruz, E. Local political institutions and smart growth. Urban Aff. Rev. 2009, 45, 218–246.

11. Yin, S. Exploring alternative care options for children in China: Recent developments and challenges. J. Public Child Welf. 2024, 19, 634–658.

12. Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2017). The politics of crisis management: Public leadership under pressure (2nd ed.). Cambridge University Press.

13. Peking University Yinghua Company; Peking University Legal Information Center. PKULAW Legal Database; Peking University: Beijing, China, 2023; Available online: https://www.pkulaw.com/ (accessed on 9 May 2024).

14. Okubo, Y. Bibliometric Indicators and Analysis of Research Systems: Methods and Examples; OECD Publishing: Paris, France, 1997.

15. Yang, Y. Strengthen publicity for early childhood care and education (ECCE) services to foster a child-friendly society. Beijing Obs. 2024, 32.

16. Katz-Sidlow, R.J.; Lindenbaum, Y.; Sidlow, R. Residents' attitudes toward a smartphone policy for inpatient attending rounds. J. Hosp. Med. 2013, 8, 541–542.

17. Rodríguez-Pose, A. Institutions and the fortunes of territories. Reg. Sci. Policy Pract. 2020, 12, 371–386.

18. Butkus, M.; Mačiulytė-Šniukienė, A.; Matuzevičiūtė, K.; Cibulskienė, D. What is the return on investing European Regional Development and Cohesion Funds? Difference-in-differences Estimator Approach. Ekon. Cas. 2019, 67, 647–676.

19. Foglia, F. Is smart specialisation monopolising the research on the EU cohesion policy? Evidence from a bibliometric analysis. Scientometrics 2023, 128, 1001–1021.

20. Li, X.; Huang, K.; Yang, W.; Wang, S.; Zhang, Z. On the Convergence of FedAvg on Non-IID Data. arXiv 2019, arXiv:1907.02189.

21. Ederveen, S.; Gorter, J.; Mooij, R.; Nahuis, R. Funds and Games: The Economics of European Cohesion Policy; CPB Netherlands' Bureau for Economic Policy Analysis: The Hague, The Netherlands, 2003.

22. Veneri, P.; Diaz Ramirez, M.; Kleine-Rueschkamp, L. Does European Cohesion Policy affect Regional Business Dynamics? Investig. Reg. J. Reg. Res. 2023, 57, 5–31.