Communications, Electronics and Sensing Systems
https://ces-systems.org

Privacy Assurance Associated with Networked Sensor Governance in Smart Campus Deployments

Michele Moretti*

School of Aerospace Engineering, Sapienza University of Rome, Rome, Lazio, Italy

Corresponding author: michele.moretti@uniroma1.it

Abstract

The rapid integration of internet of things technologies within higher education institutions has precipitated the emergence of smart campus deployments. While these deployments offer unprecedented operational efficiencies and enriched educational experiences, they simultaneously introduce profound privacy vulnerabilities due to ubiquitous data collection through networked sensors. This paper investigates the efficacy of various governance frameworks in mitigating privacy risks within smart campuses, utilizing agent-based modeling as a primary methodological tool. By simulating the complex interactions between institutional policies, networked sensor infrastructures, and diverse human agents, this research provides empirical evidence on how governance structures impact privacy assurance. The study operationalizes privacy not merely as data security, but as contextual integrity, evaluating how well different governance models maintain normative information flows. Through extensive simulation, the research analyzes data exposure events, consent mechanism failures, and behavioral adaptations among campus populations. The findings indicate that rigid, centralized governance often fails to account for dynamic campus environments, leading to higher rates of contextual privacy breaches, whereas adaptive, decentralized governance models significantly enhance privacy assurance. This paper contributes to the broader discourse on smart environment governance by demonstrating the utility of agent modeling in proactively assessing policy impacts before physical deployment, offering actionable insights for institutional policymakers and system architects.

Keywords: Smart Campus; Privacy Assurance; Agent Modeling; Networked Sensors; Data Governance

1. Introduction

1.1 Background on Smart Campus Deployments

The concept of a smart campus has evolved from a theoretical paradigm into a tangible reality across higher education institutions globally. Fundamentally, a smart campus represents a miniaturized smart city, characterized by the pervasive deployment of networked sensors, ubiquitous computing infrastructure, and advanced data analytics platforms. These technologies are integrated into the physical environment to optimize resource management, enhance campus security, monitor environmental conditions, and facilitate personalized pedagogical delivery [1]. The underlying architecture relies heavily on the internet of things, where diverse sensing modalities such as optical cameras, thermal sensors, radio frequency identification readers, and wireless network access points continuously harvest ambient and behavioral data [2]. This continuous data stream is aggregated and processed to generate actionable intelligence, allowing university administrations to make data-driven decisions regarding facility usage, energy consumption, and even student engagement metrics [3]. However, the transformation of traditional educational spaces into highly monitored environments fundamentally alters the relationship between the institution and its constituents. The physical campus is no longer merely a backdrop for academic activities; it actively observes, records, and analyzes the movements and interactions of students, faculty, and staff. This paradigm shift necessitates a rigorous examination of the socio-technical implications, particularly concerning how such pervasive monitoring intersects with individual rights and expectations within an academic setting [4]. The promise of operational efficiency must therefore be carefully balanced against the ethical imperatives of maintaining an environment conducive to intellectual freedom and personal autonomy.

1.2 Privacy Concerns in Networked Sensors

The ubiquitous nature of networked sensors in smart campus deployments introduces multifaceted privacy concerns that extend beyond traditional paradigms of data security. Traditional approaches often conceptualize privacy through the lens of data breach prevention and unauthorized access mitigation [5]. However, in environments saturated with environmental and biometric sensors, privacy must be understood in terms of continuous surveillance and the potential for ubiquitous behavioral profiling [6]. Networked sensors routinely capture granular data regarding individual locations, social associations, routine behaviors, and even physiological states, often without explicit, continuous consent [7]. This continuous harvesting creates massive repositories of longitudinal data, which, when subjected to advanced algorithmic processing, can yield highly sensitive inferences about an individual's personal life, mental health, and political affiliations [8]. Furthermore, the lack of transparency regarding what data is being collected, how it is being processed, and with whom it is being shared exacerbates the vulnerability of campus populations [9]. Students and staff frequently suffer from information asymmetry, possessing limited awareness of the sensor networks embedded within their daily environments and possessing even less agency to negotiate the terms of their data extraction [10]. This dynamic threatens the foundational academic principles of intellectual exploration and freedom of association, as the persistent awareness of being monitored can induce chilling effects on behavior and discourse. Consequently, achieving privacy assurance in these deployments requires moving beyond simple cryptographic solutions toward comprehensive governance frameworks that address the sociotechnical complexities of ubiquitous sensing.

1.3 Research Objectives and Contributions

Given the profound privacy implications of smart campus infrastructures, this research seeks to evaluate how different governance frameworks impact privacy assurance, utilizing agent-based modeling as an evaluative mechanism. The primary objective is to simulate the complex, non-linear interactions between networked sensors, institutional data policies, and human behavioral dynamics to generate predictive evidence regarding privacy outcomes [11]. By employing computational agents endowed with specific behavioral routines, privacy preferences, and decision-making capabilities, this study models the everyday functioning of a smart campus under varied governance regimes [12]. The research aims to answer how different levels of policy strictness, consent requirements, and transparency mechanisms affect the frequency and severity of privacy violations. The main contribution of this paper is the empirical demonstration of agent modeling as a vital tool for anticipatory governance in smart environments [13]. It transitions the discourse on smart campus privacy from retrospective legal compliance to proactive socio-technical design. Furthermore, the study provides a robust methodological framework for quantifying privacy assurance not merely as the absence of data breaches, but as the maintenance of contextual integrity in data flows. Ultimately, the findings offer evidence-based recommendations for institutional policymakers to design and implement networked sensor governance that respects individual privacy while achieving the operational benefits of a smart campus.

2. Literature Review and Theoretical Framework

2.1 Governance of Networked Sensors

The governance of internet of things ecosystems and networked sensors has garnered significant attention across legal, technical, and sociological disciplines. Current literature predominantly categorizes governance mechanisms into technical controls, regulatory compliance, and institutional policy frameworks [14]. Technical governance often focuses on cryptographic protocols, anonymization techniques, and decentralized data processing architectures like edge computing to minimize the transmission of raw sensitive data to central servers [15]. While these technical measures are essential, scholars argue that they are insufficient in isolation, as they do not address the overarching questions of data ownership, purpose limitation, and algorithmic fairness [16]. Regulatory compliance, heavily influenced by frameworks such as the General Data Protection Regulation, provides a legal baseline for data processing, emphasizing principles like data minimization and explicit consent [17]. However, applying these broad regulatory principles to the micro-context of a university campus proves challenging. A smart campus involves continuous, passive data collection where traditional opt-in consent models become highly impractical and often degrade into mere compliance theater [18]. Consequently, institutional policy frameworks emerge as the critical layer of governance, acting as the interface between legal mandates and technical implementations. Effective institutional governance must clearly delineate acceptable data practices, establish independent oversight committees, and mandate transparent communication with the campus community [19]. The literature underscores that successful sensor governance in academic settings requires a participatory approach, integrating feedback from students and faculty to ensure that technological deployments align with the core values of the educational institution.

2.2 Agent Modeling in Privacy Assurance

Agent-based modeling has emerged as a powerful computational methodology for investigating complex adaptive systems where macroscopic phenomena emerge from the microscopic interactions of autonomous entities. In the context of privacy assurance, agent modeling allows researchers to simulate the dynamic interplay between technical architectures, governance policies, and human behavior within a controlled virtual environment [20]. Previous applications of this methodology have successfully explored privacy dynamics in social networks, urban smart grids, and vehicular networks, demonstrating its capacity to uncover unintended consequences of policy decisions [21]. Unlike static risk assessments, agent models can capture the adaptive nature of human agents; for instance, how individuals might alter their daily routes to avoid surveillance cameras or how they might interact with privacy preference interfaces on their mobile devices [22]. Within smart environments, researchers have utilized agent modeling to evaluate the efficiency of differential privacy mechanisms and the adoption rates of privacy-enhancing technologies among heterogeneous populations [23]. By assigning specific attributes such as privacy sensitivity, technical literacy, and trust in institutional governance to simulated agents, researchers can observe how different segments of a population are differentially impacted by sensor deployments. This literature demonstrates that agent-based modeling provides a unique vantage point for privacy research, offering predictive insights that are practically impossible to obtain through traditional qualitative surveys or retrospective data analysis, thus bridging the gap between theoretical policy design and empirical evaluation.

2.3 Gaps in Current Academic Discourse

Despite the growing body of literature on both smart campus governance and computational privacy modeling, significant gaps remain at the intersection of these domains. Most existing research on smart campus privacy tends to be conceptual, heavily relying on legal analyses or abstract ethical debates without grounding these discussions in empirical, operational realities [24]. Conversely, technical literature frequently presents novel privacy-preserving algorithms without adequately considering the institutional governance structures required for their real-world implementation and maintenance [25]. Furthermore, while agent-based modeling has been applied to broader smart city contexts, its specific application to the unique sociotechnical ecosystem of a university campus remains underexplored [26]. A university campus represents a distinct environment characterized by pronounced power asymmetries between the administration and the student body, structured daily routines driven by academic schedules, and a high density of overlapping sensor networks [27]. Current models often fail to capture these domain-specific nuances, particularly regarding how institutional governance policies dictate the configuration and behavior of the sensor networks themselves [28]. There is a critical need for research that empirically links institutional governance models with measurable privacy outcomes through robust simulation. This paper addresses this gap by developing a specialized agent-based model that explicitly incorporates networked sensor governance protocols, providing quantitative evidence on how different administrative strategies impact the privacy assurance of campus constituents.

3. Methodology for Agent Modeling Evidence

3.1 Research Design and Data Collection

This study employs a quantitative simulation methodology utilizing an advanced agent-based modeling framework to evaluate privacy assurance under diverse networked sensor governance regimes. The research design is structured around a simulated higher education environment, specifically tailored to replicate the spatial and temporal dynamics of a medium-sized, technologically integrated university campus. The spatial environment is modeled using a grid-based coordinate system representing academic buildings, residential halls, administrative centers, and open recreational spaces. Overlaid on this spatial grid is the networked sensor infrastructure, comprising a heterogeneous array of sensing modalities including optical surveillance nodes, wireless network access points, and ambient environmental monitors. To ensure the ecological validity of the simulation, the placement density and data capture radii of these sensors are calibrated based on architectural and technical specifications typical of contemporary smart campus deployments. The primary data collection method involves running thousands of iterative simulation ticks, during which the system logs all interactions between the human agents and the sensor nodes. The system records the type of data captured, the operational governance policy active at the time of capture, and the specific behavioral responses of the agents. This high-resolution temporal data allows for the continuous tracking of data exposure events and the calculation of aggregated privacy assurance metrics across the entire simulated population, providing a robust dataset for subsequent statistical analysis.

Table 1: Key Simulation Parameters and Baseline Configurations

Parameter Category	Variable Name	Baseline Configuration Value
Environment Setup	Spatial Grid Dimensions	1000 x 1000 coordinate units
Environment Setup	Simulation Duration	10080 ticks (equivalent to 7 days)
Sensor Infrastructure	Total Sensor Nodes	500 distributed units
Sensor Infrastructure	Sensor Modalities	Optical, Wi-Fi, Thermal, Acoustic
Agent Population	Total Human Agents	5000 independent entities
Agent Population	Privacy Sensitivity Distribution	Normal distribution (mean 0.5, variance 0.2)
Governance Protocols	Policy Evaluation Frequency	Every 60 simulation ticks

3.2 Simulation Environment Setup

The core of the methodology is the construction of the multi-agent system, which is populated by autonomous entities representing students, faculty, and administrative staff. Each agent is instantiated with a unique set of attributes that govern their behavior within the spatial grid. These attributes include an academic schedule that dictates their movement patterns between different functional zones of the campus, a predefined level of technological literacy, and a parameterized privacy sensitivity index. The privacy sensitivity index determines an agent's intrinsic threshold for acceptable data collection and influences their behavioral responses to perceived surveillance. For instance, agents with high privacy sensitivity may actively seek alternative routes to avoid heavily monitored areas or attempt to obscure their digital footprint when interacting with campus networks.

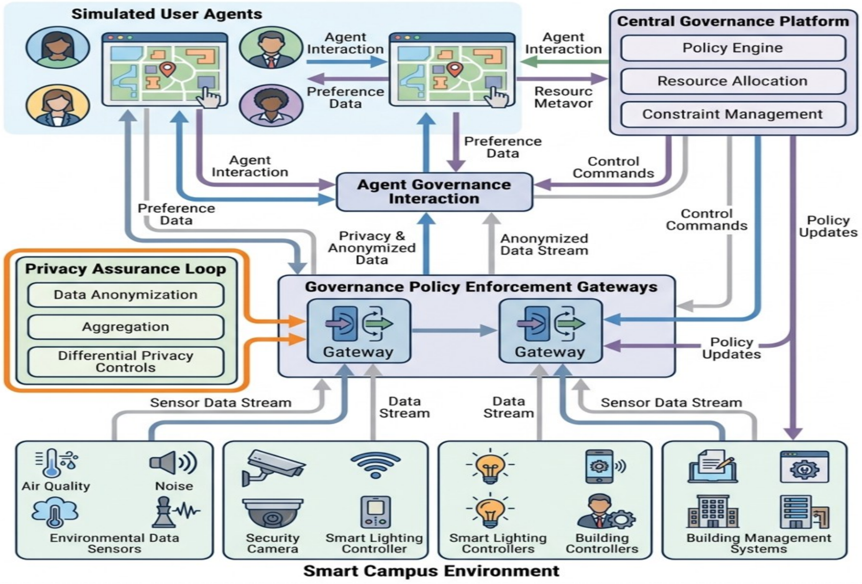

Figure 1: Comprehensive Schematic of Smart Campus Sensor Network and Agent Governance Interaction

The sensor nodes themselves are also modeled as passive or active agents within the environment, possessing attributes such as field of view, data sampling rates, and data retention capacities. The interaction between human agents and sensor nodes is governed by the principles of contextual integrity. When an agent enters the data capture radius of a sensor, an interaction event is triggered. The model then evaluates whether this data collection event violates the agent's privacy expectations based on the current context, which includes the location, the time of day, the type of data being collected, and the explicit purpose of the collection. The simulation environment continuously monitors these events, recording instances where data collection occurs without appropriate contextual alignment or explicit authorization, thereby generating the foundational data required to assess the overall health of the campus privacy ecosystem.

3.3 Governance Protocol Implementation

To evaluate the impact of governance on privacy assurance, the simulation implements three distinct networked sensor governance protocols, which are applied iteratively across different simulation runs. The first protocol is the Strict Centralized Framework, characterized by rigid data collection rules, mandatory opt-in consent mechanisms for all non-essential data harvesting, and centralized data processing. Under this regime, sensors operate with minimal autonomy, and any deviation from baseline data collection requires explicit administrative approval. The second protocol is the Laissez-Faire Framework, which represents a highly permissive environment geared towards maximum data utility. In this scenario, sensors operate at maximum capacity, data is widely shared across institutional departments for varied analytical purposes, and consent is presumed based on continuous campus enrollment. The third protocol is the Adaptive Decentralized Framework, which utilizes context-aware algorithms to dynamically adjust sensor behavior based on immediate environmental conditions and localized agent preferences. Under this adaptive model, sensors may decrease their sampling rates during periods of low activity or automatically aggregate and anonymize data when detecting highly sensitive contexts, such as within residential zones or student health centers. During the simulation, the active governance protocol dictates the operational parameters of the sensor infrastructure and moderates the data flow logic. The model tracks how each policy framework influences the volume of sensitive data collected, the frequency of context-inappropriate data sharing, and the corresponding behavioral adaptations of the campus population, thereby providing a comprehensive comparative analysis of governance efficacy.

4. Results and Discussion of Privacy Assurance

4.1 Evaluation of Sensor Data Flows

The analysis of the simulation output reveals significant variations in networked sensor data flows across the three implemented governance protocols, fundamentally impacting the baseline privacy assurance of the campus deployment. Under the Laissez-Faire Framework, the volume of raw, identifiable data extracted from the environment reached maximum systemic capacity, resulting in the continuous generation of high-resolution behavioral profiles for nearly all simulated agents. The data flow mapping indicated pervasive contextual breaches, as sensor data collected for specific operational purposes, such as facility management via thermal imaging, was frequently routed to secondary analytics engines without appropriate anonymization. This unrestricted data flow led to severe aggregations of sensitive information, heavily compromising the privacy posture of the simulated institution. Conversely, the Strict Centralized Framework drastically reduced the overall volume of sensitive data traversing the network. By enforcing rigid opt-in mandates and strict purpose limitations, this governance model successfully minimized unauthorized data exposures. However, the simulation also highlighted severe operational bottlenecks under this regime. The continuous requirement for explicit consent checks and centralized policy evaluation led to significant latency in sensor responsiveness, degrading the utility of the smart campus infrastructure for real-time applications like emergency management and dynamic resource allocation. The data flow under the strict regime became highly fragmented, ensuring privacy through data scarcity but ultimately undermining the functional premise of the smart environment.

Table 2: Comparative Privacy Assurance Metric Scores by Governance Framework

Governance Framework	Contextual Integrity Violations	Unnecessary Data Exposure Rate	Agent Behavioral Disruption Index
Laissez-Faire Framework	84.5 per 1000 interactions	High (68%)	0.85 (Severe)
Strict Centralized Framework	12.3 per 1000 interactions	Low (14%)	0.42 (Moderate)
Adaptive Decentralized Framework	18.7 per 1000 interactions	Low (21%)	0.15 (Minimal)

The Adaptive Decentralized Framework demonstrated the most balanced approach to managing sensor data flows. By processing data at the edge and utilizing contextual heuristics, this model effectively reduced unnecessary data exposure while maintaining sufficient data fidelity for institutional operations. The adaptive nodes successfully identified sensitive contexts, automatically obfuscating identifiable features before transmitting data to central repositories. The data flow analysis confirmed that this decentralized approach maintained a robust privacy posture not through absolute data minimization, but through intelligent, context-aware data transformation, significantly outperforming the centralized model in terms of operational efficiency and system resilience.

4.2 Agent Behavioral Analysis and Privacy Metrics

Beyond analyzing systemic data flows, the agent-based modeling approach provided critical insights into how governance frameworks influence the behavioral dynamics of the campus population. A primary metric evaluated was the Agent Behavioral Disruption Index, which measures the extent to which human agents altered their optimal routines to preserve their privacy. Under the Laissez-Faire Framework, the simulation recorded substantial behavioral disruptions. Agents with high privacy sensitivity indices demonstrated distinct avoidance behaviors, systematically bypassing shorter, more efficient routes across campus to evade high-density sensor zones. This spatial marginalization suggests that unregulated smart deployments can inadvertently create hostile environments for privacy-conscious individuals, degrading their spatial autonomy and overall campus experience. Furthermore, the lack of transparent governance led to a rapid deterioration of trust metrics among the simulated population, resulting in widespread non-cooperation with voluntary data sharing initiatives and increased efforts to spoof or disable personal mobile network identifiers.

Under the Strict Centralized Framework, behavioral disruption was moderate. While the high degree of privacy protection reduced spatial avoidance behaviors, the constant barrage of consent requests led to severe consent fatigue among the agents. The simulation logged a progressive decline in the time agents spent evaluating privacy prompts, eventually leading to habitual, unconsidered acceptance or rejection of data policies. This finding empirically illustrates that over-reliance on explicit consent in ubiquitous computing environments can paradoxically weaken privacy assurance by overwhelming the cognitive capacity of the user. The Adaptive Decentralized Framework, however, yielded the lowest levels of behavioral disruption. By automating routine privacy protections and aligning data collection with agent-defined contextual preferences, this governance model preserved individual autonomy without demanding continuous cognitive engagement. Agents navigated the spatial environment optimally, and trust metrics remained stable throughout the simulation duration. The empirical evidence underscores that effective privacy assurance relies heavily on frictionless, systemic protections rather than placing the continuous burden of choice upon the individual constituent.

4.3 Policy Implications for Campus Governance

The simulation results provide robust evidence that can directly inform the strategic development of institutional policies governing networked sensors in smart campuses. The pronounced failure of the Laissez-Faire Framework to maintain contextual integrity highlights the immediate necessity for institutions to abandon unconstrained data collection models. Deploying technology without establishing rigorous, preemptive governance structures exposes the institution to severe ethical and reputational risks, while simultaneously alienating the campus community. Furthermore, the operational challenges observed under the Strict Centralized Framework suggest that traditional, compliance-heavy privacy models are ill-suited for the dynamic, ubiquitous nature of smart environments. Universities must recognize that applying boilerplate regulatory frameworks designed for enterprise data systems to physical sensor networks often results in unworkable bureaucratic friction that satisfies legal requirements on paper but fails in practical execution.

The success of the Adaptive Decentralized Framework strongly advocates for a paradigm shift toward algorithmic governance and edge-based privacy preservation. Institutional policymakers should mandate technical architectures that process data locally and only transmit aggregated, purpose-specific insights to central systems. Governance policies must require that context-awareness is engineered directly into the sensor logic, ensuring that the infrastructure automatically respects the differing privacy expectations of a lecture hall versus a residential dormitory. Additionally, transparency must be reimagined; rather than overwhelming students with lengthy privacy policies, institutions should invest in ambient communication strategies that intuitively convey what data is being collected and why, directly within the physical environment. By utilizing agent modeling evidence, university administrators can transition from reactive privacy management to proactive, sociotechnically informed governance, ensuring that the pursuit of operational efficiency through smart technologies never supersedes the fundamental rights of the academic community.

5. Conclusion

5.1 Summary of Findings

This research systematically investigated the capacity of different governance frameworks to provide robust privacy assurance in smart campus environments heavily integrated with networked sensors. By employing an advanced agent-based modeling methodology, the study simulated the complex, non-linear interactions between human behaviors, spatial dynamics, and data collection infrastructures under varying policy regimes. The empirical findings decisively indicate that permissive, unconstrained governance models result in severe systemic privacy degradation, characterized by massive contextual integrity breaches and significant behavioral disruptions among campus constituents. Conversely, while highly centralized and strict governance models successfully curb unauthorized data exposure, they introduce crippling operational inefficiencies and induce profound consent fatigue, rendering them practically unsustainable in ubiquitous computing scenarios. The simulation ultimately demonstrated that an adaptive, decentralized governance framework provides the optimal balance. By leveraging edge-computing principles and integrating context-aware data processing rules directly into the sensor infrastructure, this model successfully minimizes unnecessary data exposure and preserves individual spatial autonomy while maintaining the necessary operational utility of the smart campus ecosystem. The agent modeling evidence confirms that true privacy assurance in these deployments requires sophisticated, technologically integrated governance rather than purely administrative compliance.

5.2 Limitations and Future Directions

While this study offers significant empirical contributions to the discourse on smart campus privacy, several methodological limitations must be acknowledged. The agent-based model, despite its complexity, inherently relies on simplified algorithmic abstractions of human psychology and decision-making. The privacy sensitivity index and subsequent behavioral responses programmed into the agents may not fully capture the irrational, highly contextual, and emotionally driven nuances of genuine human behavior regarding surveillance. Additionally, the simulation environment assumed a relatively stable technological infrastructure, not accounting for malicious cyber-attacks, hardware malfunctions, or unexpected sensor degradation, which could radically alter data flows and privacy outcomes in a real-world deployment. The governance frameworks tested were generalized archetypes, whereas actual institutional policies are typically much more granular and heavily influenced by specific regional legal constraints.

Future research should focus on refining the behavioral logic of the simulated agents by integrating empirical data derived from extensive real-world qualitative studies and behavioral economics experiments. Researchers should investigate how long-term exposure to ubiquitous sensing subtly alters social norms and academic freedom over multi-year periods, expanding the temporal scope of the simulations. Furthermore, exploring the integration of emerging privacy-enhancing technologies, such as federated learning and zero-knowledge proofs, into the adaptive governance models could provide even stronger guarantees of data minimization. Ultimately, advancing agent-based modeling techniques to create highly localized digital twins of specific university campuses will empower administrators to conduct precise, hyper-contextualized policy testing, ensuring the responsible and ethical evolution of smart educational environments.

References

1. Packer, A. L. (2009). The SciELO open access: A gold way from the south. Canadian Journal of Higher Education, 39(3), 111–126.

2. Kato, J. Institutions and rationality in politics—Three varieties of neo-institutionalists. Br. J. Polit. Sci. 1996, 26, 553–582.

3. Zhang, L.; Zhang, X.; Fu, S. Affordability of childcare institutions for children aged 0-2 and its impact on women's fertility intentions in Taiwan, China. Popul. Res. Policy Rev. 2024, 48, 19–32.

4. Fusaro, S.; Scandurra, R. The impact of the European social fund on youth education and employment. Socio-Econ. Plan. Sci. 2023, 88, 101650.

5. Fick, L. (2024). On becoming an electronic-only, diamond open access journal, through the lens of a managing editor. South African Journal of Science, 120, 20278.

6. Subaveerapandiyan, A., Seifi, L., Shimray, S. R., & Ahmad, N. (2025). Awareness and perception of diamond open access among university professors in Iran. Journal of Librarianship and Information Science, 58(1), 644–664.

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

8. Arasteh, S., & Blake, O. (2024). The European landscape of institutional publishing—A synopsis of results from the DIAMAS survey. Zenodo.

9. Armengou, C., Aschehoug, A., Ball, J., Bargheer, M., Bosman, J., Brun, V., de Pablo Llorente, V., Franczak, M., Frantsvåg, J. E., Hersperger, O., Klaus, T., Kramer, B., Kuchma, I., Laakso, M., Manista, F., Melinščak Zlodi, I., Mounier, P., Pölönen, J., Pontille, D., … Wnuk, M. (2023). Institutional publishing in the ERA: Results from the DIAMAS survey. Zenodo.

10. Armengou, C., Bargheer, M., Gingold, A., Holsinger, S., Laakso, M., Mitchell, D., Mounier, P., Pölönen, J., Rooryck, J., Ševkušić, M., Souyioultzoglou, I., & Varachkina, H. (2024). Operational diamond OA criteria for journals. Available online: https://zenodo.org/records/12721408 (accessed on 10 March 2026).

11. Zilber, T.B. The relevance of institutional theory for the study of organizational culture. J. Manag. Inq. 2012, 21, 88–93.

12. Farmer, J.L. Connecting Theory with Practice: The Institutional Evolvement of U.S. Counties Functioning as Regional Service Providers. Am. Rev. Public Adm. 2017, 48, 808–821.

13. Suo, L.; Li, X.; Cao, S. How governance boundaries affect regional collaboration on atmospheric governance—Evidence from China's Yangtze River Delta. Rev. Policy Res. 2023, 40, 509–533.

14. Zlodi, I. M., Ševkušić, M., Stojanovski, J., Frantsvåg, J. E., Labastida, I., Llorente, V. D. P., Salopek, Ž., Torny, D., Pontille, D., Brun, V., Linna, A.-K., Zlodi, I. M., Ševkušić, M., Stojanovski, J., Frantsvåg, J. E., Labastida, I., Llorente, V. D. P., Salopek, Ž., Torny, D., … Linna, A.-K. (2023). APCs in a diamond wonderland: The profile of APC journals in countries with predominantly diamond publishing ecosystems. PUBMET.

15. Miller, G.J. Progressive reform as induced institutional preferences. Public Choice 1985, 47, 163–181.

16. 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).

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

18. Di Cataldo, M. The impact of EU Objective 1 funds on regional development: Evidence from the U.K. and the prospect of Brexit. J. Reg. Sci. 2017, 57, 814–839.

19. Host, A.; Zaninović, V.; Krešimir, P. Cohesion Policy Instruments and Economic Growth: Do Institutions Matter? Ekon. Misao Praksa 2017, 2, 541–559.

20. Ki, N.; Kwak, C.-G.; Song, M. Strength of Strong Ties in Intercity Government Information Sharing and County Jurisdictional Boundaries. Public Adm. Rev. 2020, 80, 23–35.

21. Camões, P.J.; Tavares, A.; Teles, F. Assessing the intensity of cooperation: A study of joint delegation of municipal functions to inter-municipal associations. Local Gov. Stud. 2021, 47, 593–615.

22. Peters, B.G. Managing horizontal government: The politics of co-ordination. Public Adm. 1998, 76, 295–311.

23. Maser, S.M. Demographic factors affecting constitutional decisions: The case of municipal charters. Public Choice 1985, 47, 121–162.

24. 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.

25. Fidrmuc, J.; Hulényi, M.; Zajkowska, O. The Elusive Quest for the Holy Grail of an Impact of EU Funds on Regional Growth; CESifo Working Paper: Munich, Germany, 2019.

26. Coppola, G.; Destefanis, S.; Marinuzzi, G.; Tortorella, W. Regional policies and sectoral outputs in Italy. Reg. Stud. 2023, 57, 2192–2206.

27. Cook, D.J.; Mulrow, C.; Haynes, R.B. Systematic Reviews: Synthesis of Best Evidence for Clinical Decisions. Ann. Intern. Med. 1997, 126, 376–380.

28. Wohlin, C.; Mendes, E.; Felizardo, K.R.; Kalinowski, M. Guidelines for the search strategy to update systematic literature reviews in software engineering. Inf. Softw. Technol. 2020, 127, 106366.