Hyperconnected horizons: decoding the digital sovereignty of european smart cities

Adrian-Victor VEVERA,
National Institute for Research and Development in Informatics, ICI-Bucharest, Romania,
victor.vevera@ici.ro

Ulpia-Elena BOTEZATU,
National Institute for Research and Development in Informatics, ICI-Bucharest, Romania,
ulpia.botezatu@ici.ro

Abstract
This article explores the intersection of governance policies and technological advancements in the context of smart cities, engaging with the entwined concepts of smart cities and digital sovereignty within the European landscape. Employing a poststructuralist lens, it critically examines the ramifications of stringent regulations on the incorporation of innovative technologies in smart cities. The analysis navigates divergent national perspectives, emphasizing the tension between digital sovereignty and an open-market ethos. Through nuanced exploration and case studies, the article seeks to unravel the complexities inherent in reconciling these paradigms, offering insights for policymakers, urban planners, and technology stakeholders navigating the intricate terrain of Smart City development amid Europe's pursuit of digital sovereignty. This succinct exploration contributes to academic discourse by fostering a critical dialogue around the intersectionality of technological innovation, governance, and urban development within the contemporary European context.

Keywords: digital sovereignty, smart cities, smart governance, ICT, technological innovation.

1. Introduction
The rapid advancement of the digital era has brought about significant changes in urbanization, giving rise to smart cities that utilize advanced technologies to optimize efficiency, sustainability, and the well-being of citizens. In the European context, the concept of digital sovereignty and its implications for cloud services has emerged as a crucial topic of discussion [1, 2]. The proposed Cybersecurity Certification Scheme for Cloud Services in Europe [3] serves as a focal point, driving a complex interplay between commercial and political dynamics.

Against this backdrop, major American technology companies, such as Amazon Web Services, Microsoft, and Oracle, have introduced customized cloud solutions designed specifically for the European market. These initiatives aim to address European concerns about data localization and exemplify the desire for digital autonomy [4]. This paper aims to rigorously examine the multifaceted aimplications that arise from the proposed European cybersecurity certification framework [5, 6]. It seeks to contextualize this framework within the intricate nexus of digital sovereignty, cloud infrastructure, and the evolving nature of Smart City development.

The core of this examination lies in the exploration of divergent national perspectives, particularly observed in the contrasting attitudes of France and Germany. France advocates for strict controls on non-European cloud providers, while Germany favors a more open-market approach. A thorough analysis is required to understand the complexities surrounding the proposed certification's scope, as it extends beyond the realm of

government to various commercial sectors. This analysis reveals that the discourse on this topic transcends technological considerations, encompassing broader geopolitical dimensions and creating significant tensions between digital autonomy and global market dynamics.

Furthermore, this paper seeks to move beyond a descriptive account of the topic and instead offers a critical evaluation of the ongoing debate. Utilizing a poststructuralist lens, the objective is to uncover the underlying discursive elements and examine how stringent regulations embedded within the certification framework might impede the seamless integration of innovative technologies critical for the advancement of smart cities. The resulting tension between digital sovereignty and an open-market ethos becomes a testing ground for the feasibility of Europe's pursuit of enhanced Smart City development.

Positioned at the confluence of technological innovation, governance mandates, and expanding urban networks, this investigation aspires to make a substantial contribution to the scholarly conversation around the synergy of digital sovereignty and Smart City evolution in the modern European context. Through the lens of empirical case studies and thorough analytical scrutiny, this paper offers fresh perspectives that challenge established narratives. It aims to provide a scholarly foundation for decision-makers, urban strategists, and technology stakeholders as they navigate the intricate challenges of fostering Smart City growth amidst Europe's relentless pursuit of digital autonomy.

In the subsequent sections, we embark on a comprehensive exploration of the European Cybersecurity Certification Scheme for Cloud Services. By dissecting its implications across multiple dimensions, we navigate through the evolving landscape of digital governance, technological innovation, and urban development.

2. Global context of digital sovereignty

In the modern era of information technology, the concept of digital sovereignty plays a pivotal role in shaping the discourse surrounding data governance and cyber autonomy [7]. Digital sovereignty represents the ability of nations or entities to maintain control and autonomy over their digital infrastructures, data flows, and information systems [8]. It mirrors the interplay between technological advancements, geopolitical factors, and the imperative to protect national interests in an increasingly interdependent world.

The genesis of digital sovereignty can be traced to the growing recognition of the vital role that digital assets play in economic, political, and societal domains. As information and communication technologies permeate every aspect of contemporary existence, the establishment and preservation of digital sovereignty become imperative. This recognition is reinforced by the increasing frequency and sophistication of cyber threats, necessitating strategic measures to enhance the resilience of nations against potential vulnerabilities in their digital ecosystems [6, 5].

In the European context, the principles of digital sovereignty gain enhanced significance, particularly with the rise of smart cities [9]. Smart cities represent the convergence of urban infrastructure and cutting-edge technologies, serving as hubs of innovation and efficiency

[10]. Digital sovereignty becomes essential to ensuring the integrity, security, and ethical utilization of data within these technologically-driven urban ecosystems.

As European nations advance their smart city projects, they encounter the intricate challenge of balancing technological innovation with the preservation of digital autonomy [11]. This concept of digital sovereignty transcends conventional cybersecurity approaches, enveloping a broader spectrum of strategic decisions encompassing data governance, infrastructural technology, and the cultivation of homegrown technological proficiencies. The complex interrelation between digital sovereignty and the evolution of smart cities in Europe necessitates a delicate equilibrium—leveraging global technological developments while protecting the unique values and interests of individual nations [12].

To adeptly traverse this convoluted terrain, a comprehensive understanding of the global context of digital sovereignty is indispensable. Grasping the multifaceted aspects of this concept lays the groundwork for appreciating the intricate dynamics at play, particularly in relation to the anticipated impact of cybersecurity certification schemes on cloud services and the overarching theme of digital sovereignty within the European framework.

2.1. Enhancing cybersecurity measures and strengthening cloud services in Europe

Digital governance in the European Union is currently focused on bolstering cybersecurity measures and ensuring the integrity of cloud services. One notable initiative driving this agenda is the proposed Cybersecurity Certification Scheme for Cloud Services [13]. This strategic effort aims to enhance the security protocols surrounding digital infrastructure in Europe, with a particular emphasis on safeguarding critical data against potential threats.

Moreover, recent initiatives undertaken by prominent American cloud service providers further highlight the dynamic nature of this discourse. Microsoft's “Cloud for Sovereignty” exemplifies their proactive approach, demonstrating an understanding of the evolving digital landscape and a commitment to aligning cloud services with European aspirations for digital autonomy [14]. Similarly, Oracle's “EU Sovereign Cloud” reflects their conscious effort to cater to the unique regulatory demands and security considerations prevalent within the European Union.

These initiatives by American tech giants respond to the increasing concerns within the European community regarding data sovereignty. As the European Union deliberates on comprehensive cybersecurity certification protocols, the strategic positions taken by major American corporations add complexity to the overall discourse [15]. This intersection between the proposed European scheme and the autonomous initiatives of American corporations represents a significant area where divergent ideologies surrounding digital governance and sovereignty converge.

In summary, the examination of current initiatives in Europe reveals a multifaceted landscape characterized by the interplay of regulatory frameworks and corporate strategies. This analysis serves as a foundational exploration into the evolving dynamics of digital sovereignty and cybersecurity within the context of European smart cities. It provides valuable insights into the broader implications on both regional and global scales.

2.2. Commercial and political battles in european digital policy

A heated dispute has unfolded among key European Union member states, especially France and Germany, over the crucial issues of digital sovereignty and the utilization of external cloud services. This complex issue showcases the interplay between economic imperatives and governmental principles within the broader context of European digital policy.

At the heart of the debate are divergent national perspectives on digital sovereignty and the role of non-European cloud providers. France, firm in its stance to protect its digital autonomy, urges for limitations on the influence of non-European cloud service providers, particularly those from the United States. This approach is in line with France's historical commitment to promoting national champions and maintaining control over strategic technological domains [16].

Conversely, Germany, a key player in the European Union, has adopted a stance that stands in contrast to France's position. Influenced by the Free Democratic Party's presence in key ministries in Berlin, Germany has voiced criticisms of France's push for digital autonomy and has shown support for a more open-market approach [17]. Notably, the German Federal Office for Information Security has shown favor towards initiatives such as the Amazon European Sovereign Cloud, illustrating a variance in regulatory perspectives compared to France.

The dynamics of this commercial and political tug-of-war are further complicated by the involvement of smaller EU member states, each with their own priorities and preferences. While France aims to bolster European digital capabilities through protectionist measures, smaller EU members like Estonia, the Netherlands, and Greece argue that such approaches could result in higher costs and detriment to healthy competition. These differing opinions among member states contribute to the complexity of forming a cohesive European stance on digital policy.

As a result, the disparities in national perspectives and the ensuing debates play a pivotal role in shaping the trajectory of European digital policy. The intricate interplay between commercial considerations and political ideologies adds depth to the ongoing narrative surrounding digital sovereignty, highlighting Europe's evolving position on integrating foreign cloud services into its technological landscape.

3. Exploring case studies

This section delves deeper into specific case studies, shedding light on the diverse approaches various cities have taken towards integrating cybersecurity certification initiatives into their smart city frameworks. We aim to illustrate the nuances in the implementation of digital sovereignty and cloud services adoption, underlining the unique challenges and solutions each city presents.

3.1. Barcelona, Spain – Comprehensive Smart City initiatives with digital sovereignty

Barcelona, a pioneer in smart city initiatives, has made significant strides in integrating technology into urban management. The city's approach has been multifaceted, focusing on improving public services, enhancing quality of life, and increasing urban efficiency. A

key aspect of Barcelona's strategy is its commitment to digital sovereignty, manifested through the adoption of open-source technology platforms. These platforms facilitate a transparent and secure management of citizen data, ensuring privacy and security in accordance with EU data protection standards [18]. By creating its own technology stack, Barcelona retains control over data and infrastructure, setting a benchmark for how cities can assert digital sovereignty while fostering innovation.

3.2. Estonia – A national blueprint for digital sovereignty

Estonia's journey as a digital nation is characterized by its comprehensive approach to digital governance and cybersecurity. The country's digital strategy, highlighted by the e-Estonia initiative, has been a cornerstone in establishing a secure and seamless digital society [19]. Estonia's success lies in its ability to integrate digital solutions across government services, ensuring citizen-centricity, efficiency, and security. The nation's digital sovereignty is evident in its robust data governance policies, which have enabled the development of secure digital IDs and e-services. Estonia's model demonstrates how digital sovereignty can be achieved through national strategy, offering lessons for smart city developers on integrating cybersecurity at every level of urban digital infrastructure.

3.3. Amsterdam, Netherlands – Data ethics in Smart City development

Amsterdam's smart city development is grounded in a strong commitment to data ethics and privacy. The Amsterdam Smart City initiative illustrates how urban innovation can be driven by collaboration between the public sector, private companies, and residents [20]. This approach ensures that technological advancements serve the broader community interests. Amsterdam's focus on ethical data usage, citizen engagement, and transparent governance has been crucial in maintaining digital sovereignty at the city level. This case highlights the importance of considering ethical implications in smart city development and the role of participatory governance in achieving digital autonomy.

3.4. Germany – Strategic cybersecurity and cloud computing development

Germany's approach to cybersecurity and cloud computing showcases a national strategy that balances open-market principles with digital sovereignty. The development of Gaia-X, a project aimed at creating a secure and competitive European cloud infrastructure, is indicative of Germany's commitment to technological self-reliance [21]. This initiative not only enhances Germany's digital infrastructure but also contributes to the broader European digital ecosystem. Germany's strategy underlines the potential for large economies to develop indigenous technological solutions while maintaining active participation in international collaborations and markets.

The exploration of these case studies — Barcelona, Estonia, Amsterdam, and Germany — provides a comprehensive view of the varied approaches to digital sovereignty and cybersecurity in smart city development. Each case study demonstrates unique strategies and solutions, reflecting the specific contexts and priorities of the respective cities and country. While Barcelona and Amsterdam focus on city-level initiatives, Estonia and Germany present national strategies that offer insights into broader policy frameworks. These diverse experiences contribute valuable lessons for cities and nations worldwide, highlighting the importance of customized approaches to digital governance in the era of smart cities.

4. Global community response

Evaluating the international community's reaction, particularly the positions expressed by the United States, Japan, and other non-European governments, towards the proposed European cybersecurity certification initiatives is of significant import within this discourse. An in-depth examination of these global perspectives is crucial for understanding the wider implications and potential diplomatic consequences of Europe's pursuit of digital sovereignty.

An analysis of the United States' standpoint uncovers notable concerns and reservations, evident in high-level diplomatic interactions. In a communication exchange between U.S. Trade Representative Katherine Tai and European Commission Executive Vice President for trade Valdis Dombrovskis, apprehensions regarding the French and EU cybersecurity certification schemes were articulated. The issue has escalated to a formal concern within the U.S. government, as highlighted by Kenneth Propp from the Atlantic Council.

Simultaneously, the responses from non-European nations, including Japan, add to the multifaceted global dynamics surrounding this issue. Comprehending their perspectives and potential objections is crucial for grasping how Europe's pursuit of enhanced cybersecurity measures is perceived beyond its borders.

Moreover, the involvement of international organizations and trade councils in this ongoing dispute introduces additional complexity to the discussion. These entities play a critical role in mediating and influencing global trade dynamics, and their participation in deliberations on European cybersecurity certification introduces another layer of complexity to the geopolitical implications. Examining the positions taken by such organizations provides valuable insights into the broader diplomatic landscape, shedding light on potential consequences and alliances formed in response to Europe's ambitions for digital sovereignty.

In summary, the international community's response to European cybersecurity certification proposals encompasses a complex interplay of diplomatic, economic, and strategic considerations. Analyzing the positions of key global actors and the involvement of influential international organizations is essential for gaining a nuanced understanding of the broader implications of Europe's efforts in digital governance and cybersecurity.

5. Economic and technological implications

Understanding the economic and technological impact of embracing or rejecting the proposed cybersecurity certification is crucial for the European landscape. This section conducts an in-depth assessment of the multifaceted consequences, examining both the economic and technological dimensions involved in the decision-making process of the certification framework.

To fully grasp the economic implications, a detailed analysis is undertaken to determine the potential outcomes that may arise from either adopting or dismissing the proposed cybersecurity certification. This evaluation encompasses a range of factors, including market dynamics, trade dependencies, and the overall financial well-being of the European

Union. The aim is to illuminate how the certification framework may influence the economic equilibrium, assessing whether the proposed measures promote resilience or pose potential disruptions to the economic structure of the region.

Simultaneously, this section explores the technological repercussions resulting from strategic choices made regarding cloud services and digital sovereignty. By analyzing the intricate relationships between technological infrastructure, data governance, and security protocols, the discussion seeks to reveal hidden consequences. It delves beyond immediate technological considerations to consider the broader scope of innovation, research and development, and the overall trajectory of technological advancement within the European smart city model.

Through this comprehensive exploration, the section provides a scholarly perspective that extends beyond a surface-level analysis, offering nuanced insights into the complex web of consequences that European stakeholders face in the evolving landscape of digital sovereignty and smart city development.

6. Conclusions and future perspectives

To conclude, this paper has diligently examined the complex interplay between digital sovereignty, cloud services, and the evolving landscape of smart cities in Europe. Key findings highlight the critical importance of addressing the tensions that arise from the convergence of national digital autonomy and the use of cloud infrastructure provided by non-European entities.

A comprehensive recapitulation of these findings emphasizes the multifaceted challenges encountered by European policymakers, urban planners, and technology stakeholders. The commercial and political complexities epitomized by the divergent positions of member states, particularly France and Germany, underscore the intricacies involved in reconciling aspirations for digital sovereignty with the principles of an open market.

As we navigate the dynamic terrain of contemporary smart city development, it is crucial to reflect not only on the current state but also to envisage the future. Based on the analysis presented, it is recommended that Europe's digital policy incorporates a balanced approach that fosters domestic technological capabilities while embracing global innovation. Future directions should carefully consider the economic, technological, and geopolitical implications inherent in these policy decisions.

Moreover, the evolution of smart cities necessitates a proactive engagement with emerging technologies, acknowledging the ever-changing nature of the digital landscape. As Europe strives to assert its digital sovereignty, it should envision a progressive and forward-thinking policy framework that protects national interests and facilitates the integration of cutting-edge technologies into urban environments.

In essence, this paper serves as a foundation towards a deeper understanding of the intricate dynamics shaping the digital future of European smart cities. The suggestions offered herein contribute to the ongoing discourse surrounding the delicate balance between digital

autonomy and international collaboration. They provide a scholarly foundation for future investigations into digital policy and the evolution of smart cities within the European context.

References

[1] F. Bélanger and R. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly,* vol. 35, no. 4, pp. 1017-1041, 2011.

[2] R. Kitchin, "The ethics of smart cities and urban science," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences,* vol. 374, 2016.

[3] European Commission, "EU Cloud Certification Scheme," 9 June 2021. [Online]. Available: https://ec.europa.eu/newsroom/cipr/items/713799/en. [Accessed 4 December 2023].

[4] R. Giffinger, C. Fertner, H. Kramar, R. Kalasek, N. Pichler-Milanović and E. Meijers, "Smart cities: Ranking of European medium-sized cities," Centre of Regional Science (SRF), Vienna University of Technology, Viena, Austria, 2007.

[5] EU Commission, "The EU cybersecurity certification framework," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework. [Accessed 4 December 2023].

[6] ENISA, "Cybersecurity Certification Framework," [Online]. Available: https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework. [Accessed 4 December 2023].

[7] A. Georgescu, A.-V. Vevera and C.-E. Cîrnu, "The Diplomacy of Systemic Governance in Cyberspace," *International Journal of Cyber Diplomacy,* vol. 1, no. 1, pp. 79-88, 2020.

[8] T. Porter and N. Tan, "Introduction: democracy and digitization," *Globalizations,* vol. 20, no. 1, pp. 132-136, 2023.

[9] A. Savin, "Digital Sovereignty and its Impact on EU Policymaking," CBS LAW Research Paper No. 22-02, Copenhagen Business School, Denmark, 2022.

[10] A. Vito, U. Berardi and R. Dange, "Smart cities: definitions, dimensions, and performance," *Journal of Urban Technology,* vol. 22, no. 1, 2015.

[11] U.-E. Botezatu, O. Bucovetchi, Gheorghe, A.V. and R. Stanciu, "Strengthening Urban Resilience: Understanding the Interdependencies of Outer Space and Strategic Planning for Sustainable Smart Environments," *Smart Cities,* vol. 6, pp. 2499-2518, 2023.

[12] E. Morozov and F. Bria, Rethinking the Smart City: Democratizing Urban Technology, New York: Rosa Luxemburg Stiftung, 2018.

[13] "European Cloud Strategy," 27 September 2012. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF. [Accessed 4 December 2023].

[14] L. Carter and J. Ubacht, "Blockchain applications in government," in *1-2. 10.1145/3209281.3209329*, 2018.

[15] "European cybersecurity reglation takes a soveregn turn," 13 September 2022. [Online]. Available: https://www.crossborderdataforum.org/european-cybersecurity-regulation-takes-a-sovereign-turn/. [Accessed 4 December 2023].

[16] "French Cybersecurity Agency," [Online]. Available: https://cyber.gouv.fr/en. [Accessed 4 December 2023].

[17] "Germany calls for political discussion on EU's cloud certification scheme," 21 September 2022. [Online]. Available: https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/. [Accessed 4 December 2023].

[18] "Barcelona City Council will have a pioneering municipal AI strategy in Europe," [Online]. Available: https://citiesfordigitalrights.org/barcelona-city-council-will-have-pioneering-municipal-ai-strategy-europe. [Accessed 4 December 2023].

[19] "We have built a digital society and we can show you how," [Online]. Available: https://e-estonia.com/. [Accessed 4 December 2023].

[20] "Amsterdam Smart city," [Online]. Available: https://wwf.panda.org/es/?204657/Amsterdam-Smart-city. [Accessed 4 December 2023].

[21] "Gaia-X," [Online]. Available: https://gaia-x.eu/. [Accessed 4 December 2023].