TechHub Journal Vol. 3, pp. 74-80 (2024)
ISSN: 2810-2800
www.techhubresearch.com

Public Policies in Data Security in the European Union: A Literature Review

Gherghin Claudia-Anamaria

Master's student in Public Institutions Management, Faculty of Law and Administrative Sciences, Ovidius University of Constanța

claudia.gherghin@yahoo.com

Abstract. This literature review explores the multifaceted development of public policies in data security within the European Union. It synthesizes findings from fourteen key academic studies and policy analyses, identifying challenges such as regulatory fragmentation, ethical governance, technological uncertainties with blockchain, and the pursuit of digital sovereignty. The analysis reveals that harmonized regulations are needed to bridge gaps across diverse sectors like finance, aviation, and critical infrastructure. Ethical considerations surrounding AI, algorithmic decision-making, and data sharing emerge as essential for fostering public trust. The review also examines institutional dynamics, highlighting the roles of ENISA, national agencies, and EU legislative initiatives like the Digital Operational Resilience Act. It discusses how political negotiations and sector-specific needs complicate the path toward a unified cybersecurity framework. The synthesis underscores the importance of balancing innovation with compliance, safeguarding citizens' rights while promoting technological advancement. Ultimately, the review advocates for a more integrated, ethical, and resilient policy landscape and suggests areas for future research, emphasizing collaboration among EU institutions, member states, industry stakeholders, and researchers to address emerging cyber threats and achieve digital sovereignty.

Keywords. data security, regulatory fragmentation, ethical governance, digital sovereignty, blockchain

Introduction

The European Union (EU) stands at the forefront of developing robust public policies to safeguard data security in an increasingly digital world. As information and communication technologies evolve rapidly, the security of data has become critical not only for protecting personal privacy and intellectual property but also for preserving the integrity of critical infrastructures, maintaining economic stability, and ensuring national and digital sovereignty. Data security policy-making in the EU involves a delicate balancing act: policymakers must address the technical complexities of emerging technologies like blockchain, artificial intelligence (AI), and cloud computing while navigating ethical concerns, legal frameworks, economic implications, and geopolitical considerations.

The development of public policies for data security in the EU is influenced by multiple factors. On one hand, it is driven by the need to create a safe digital environment that fosters innovation, supports the Digital Single Market, and ensures citizens' trust in digital

services. On the other hand, it must contend with threats from sophisticated cybercriminals, geopolitical tensions, and the challenges posed by dependencies on non-European technological providers. The pursuit of digital sovereignty, which seeks to regain control over data and digital infrastructures, has become a strategic priority for the EU (Blancato & Carr, 2024). However, this ambition often intersects with complex regulatory landscapes and institutional dynamics, as agencies like the European Union Agency for Cybersecurity (ENISA) strive to coordinate efforts across member states (Dunn Cavelty & Smeets, 2023).

Ethical considerations also play a critical role in shaping data security policies. The deployment of AI and algorithmic decision-making systems raises questions about bias, transparency, and accountability, necessitating frameworks that protect individuals' rights while promoting innovation (Akgun et al., 2024). Furthermore, the rapid advent of blockchain technology presents both opportunities and regulatory challenges, particularly concerning data immutability and compliance with the General Data Protection Regulation (GDPR) (Cagigas et al., 2021).

This literature review synthesizes insights from a range of academic studies and policy analyses, drawing on 14 key sources to explore how public policies in the EU are evolving to address data security. By integrating perspectives on regulatory fragmentation, ethical governance, technological challenges, digital sovereignty, sector-specific applications, and institutional roles, the review aims to provide a comprehensive overview of the current state of EU data security policies, the challenges they face, and potential directions for future research and policy development.

Literature review

The literature on EU data security policies is diverse, reflecting the complexity of the challenges involved in securing data across a digitally interconnected union. The following sections delve into various thematic areas highlighted by the 14 sources, integrating their findings to present a cohesive picture of the policy landscape.

Regulatory Fragmentation and Governance Challenges

A recurring concern in the literature is the fragmentation of regulatory frameworks, which undermines the effectiveness of data security policies. Akgun, Gerli, Mora, and McTigue (2024) illustrate this issue within the context of smart city implementations, noting that "inefficient regulations and guidelines on smart city technologies... fail to define clear roles and responsibilities within and across different organisations" (p. 21). This lack of clarity leads to inconsistent security practices and makes it difficult to establish a unified approach to data protection across the EU.

Such fragmentation extends beyond smart cities into various sectors, including finance, aviation, and critical infrastructure. De Gramatica et al. (2015) discuss similar challenges in the aviation sector, where cybersecurity regulations often lack a global framework and coherent risk-based approaches. Their work emphasizes the need for EU-level harmonization to address the complex interdependencies of IT systems in aviation, suggesting that "a more trans-border and inter-sectoral collaborative security regulation would be required". Without harmonized regulations, efforts to secure data and critical systems remain piecemeal, increasing the vulnerability of the entire digital ecosystem.

Ethical Considerations and Holistic Data Regulation

The ethical dimensions of data security are increasingly prominent in policy discussions. Akgun et al. (2024) highlight critiques from earlier studies that point to the "lack of ad hoc regulations to address ethical concerns in the use of algorithmic decision-making" (p. 21). As AI systems become more integrated into decision-making processes, the risk of bias, discrimination, and lack of transparency emerges, necessitating robust ethical frameworks within data security policies. These ethical considerations are not limited to AI but extend to how data is shared and managed across organizations. Akgun et al. (2024) argue that the absence of "holistic data regulations" can be a disincentive to data sharing, as organizations fear the ethical and legal repercussions of handling sensitive data improperly (p. 21).

The integration of ethical principles into public policy can build trust among citizens and institutions, encouraging collaboration and data sharing while safeguarding against misuse. This holistic approach to regulation must address not only technical vulnerabilities but also the social implications of data security measures. Policies that embed ethical guidelines can help ensure that technological advancements do not compromise fundamental rights and societal values, balancing innovation with accountability and fairness.

Blockchain Technology and Regulatory Uncertainty

Blockchain technology is lauded for its potential to enhance transparency and security through immutable ledgers. However, its adoption in public services faces significant regulatory uncertainties. Cagigas, Clifton, Diaz-Fuentes, and Fernandez-Gutierrez (2021) explore these challenges, noting that "regulatory uncertainty regarding blockchain is still a major risk" (p. 13910). The primary concern arises from the tension between blockchain's inherent immutability and legal requirements such as the GDPR's right to erasure. This conflict presents a fundamental challenge for integrating blockchain into areas where personal data is involved.

The European Blockchain Services Infrastructure (EBSI) is an example of the EU's initiative to harness blockchain while addressing its regulatory challenges. EBSI aims to create a trusted, public-permissioned blockchain infrastructure to improve services like digital identity verification, notarization, and trusted data sharing (Cagigas et al., 2021). However, realizing these goals requires establishing a regulatory environment that reconciles blockchain's technical properties with legal frameworks. This entails developing standards for interoperability, legal recognition of blockchain agreements, and mechanisms to ensure compliance with privacy laws. The tension between innovation and regulation underscores the delicate balancing act policymakers face in fostering technology adoption while safeguarding citizens' rights.

Cybersecurity Governance and Institutional Dynamics

Institutions such as the European Union Agency for Cybersecurity (ENISA) are central to shaping EU data security policies. Dunn Cavelty and Smeets (2023) provide an in-depth analysis of ENISA's evolution, noting that "ENISA struggled to become a relevant actor by carving out a specific role for itself". Their study underscores the challenges ENISA faces in asserting epistemic authority, navigating political pressures, and coordinating among diverse national frameworks. The agency's journey reflects broader themes in cybersecurity governance, where institutional legitimacy, capacity, and clear mandates are crucial for effective policy implementation. Cooperation among Member States, including structures like CERT and CSIRT under governmental oversight, is crucial for effectively defending their cyber sovereignty and implementing cohesive policies (Koulas, Shah & Peristeras, 2022).

TechHub Journal Vol. 3, pp. 74-80 (2024)
ISSN: 2810-2800
www.techhubresearch.com

Bygrave (2022) contributes to this discussion by arguing that cyber resilience should not overshadow fundamental cybersecurity objectives. He emphasizes that both goals should be pursued simultaneously within policy frameworks, suggesting that "operationalization of cyber resilience is achievable within an appropriately comprehensive 'security-by-design' framework" aligned with EU law. This integrated approach is vital for creating policies that not only prevent attacks but also ensure rapid recovery and continuity of services in the face of disruptions.

The evolution of cybersecurity governance within the EU is further complicated by the interplay between national and supranational interests. Furthermore, EU institutions not only guide but also mobilize national resources or directly produce collective security, highlighting the complex dynamics of security policy instruments in tech-driven shared security spaces (Sivan-Sevilla, 2023). Moreover, Sivan-Sevilla (2021) explores these dynamics in the context of cybersecurity certification, revealing tensions between efforts to harmonize certification processes at the EU level and national sovereignty concerns. The concept of "Europeanisation on Demand" emerges, where integration is shaped by negotiations between EU institutions and member states, each seeking to protect core state powers while advancing collective goals. These dynamics illustrate how institutional arrangements and intergovernmental negotiations influence the design and effectiveness of data security policies.

Digital Sovereignty and Cloud Computing

Digital sovereignty has become a key focus for the EU as it seeks to reduce dependency on foreign cloud providers and assert control over critical data infrastructures. Blancato and Carr (2024) discuss how the EU's push for data sovereignty is partly a response to a "trust deficit" with American hyperscalers. They explain that European governments' reliance on a few large cloud providers raises concerns about data confidentiality, availability, and control, prompting regulatory initiatives aimed at regaining sovereignty over digital infrastructures.

The pursuit of digital sovereignty has significant economic and strategic implications. On one hand, it opens up a substantial market opportunity for sovereign cloud solutions, projected to reach billions of dollars in the coming years. On the other hand, overly restrictive policies could hinder cloud adoption, limit innovation, and create barriers for international collaboration. Blancato and Carr (2024) caution that while sovereign approaches to cloud computing may enhance cybersecurity and data control, they must be balanced against potential negative impacts on economic growth and technological development.

Efforts to assert digital sovereignty involve a combination of regulatory measures, technological solutions, and strategic partnerships. These may include promoting European cloud providers, mandating data residency within the EU, implementing advanced cryptographic techniques, and establishing granular access controls to ensure data confidentiality. Rone (2024) further explores how diverging national preferences and disputed institutional competences complicate the EU's cloud sovereignty ambitions, highlighting that technological limitations and political disagreements can hinder policy implementation and the realization of a truly sovereign digital infrastructure.

Sector-Specific Challenges and Initiatives

The application of data security policies varies significantly across sectors, each with its own unique challenges and requirements. In aviation, De Gramatica et al. (2015) discuss how the lack of a global cybersecurity framework necessitates tailored, risk-based approaches to protect complex networks of airports and airlines. They emphasize the importance of

equitable cost distribution and flexible regulations that can adapt to the differing capacities of smaller and larger airports. Their recommendations for cybersecurity redistribution mechanisms underscore the interplay between economic fairness and security policy effectiveness.

In the financial sector, Donnelly, Camacho, and Heidebrecht (2024) analyze the Digital Operational Resilience Act (DORA), which aims to harmonize cybersecurity regulations for digital financial services across the EU. DORA introduces oversight of critical ICT providers, aligning financial sector regulations with broader EU cybersecurity goals and embedding resilience into the fabric of digital finance. The act reflects a growing recognition that cybersecurity is not merely an IT issue but a fundamental component of financial stability and market integrity.

Chiappetta and Cuozzo (2017) focus on critical infrastructure protection, particularly in transport sectors such as ports and airports. They highlight the necessity of stringent cybersecurity measures for firmware and the adoption of EU directives like the Security of Network and Information Systems Directive. Their work illustrates how sector-specific policies must align with broader EU standards to ensure consistent and effective protection of vital services.

Sovereign Cloud and National Preferences

Carver (2024) examines the discourse around European digital sovereignty and its implications for public policies, including cloud computing strategies. He outlines how discussions of sovereignty shape policy instruments, standard setting, and external relations. Carver underscores the role of cybersecurity as a pillar of digital sovereignty, linking initiatives like the 5G Toolbox to broader EU strategic autonomy goals.

These sector- and technology-specific discussions illustrate the intricate web of considerations that shape public policies in data security within the EU. Each reference contributes to a layered understanding of the field, revealing how regulatory fragmentation, ethical imperatives, technological innovation, institutional dynamics, and strategic ambitions intersect to influence policy outcomes.

Conclusions

The literature on EU public policies in data security paints a picture of a complex, evolving landscape. Policymakers must navigate regulatory fragmentation, ethical dilemmas, technological disruptions, and geopolitical considerations while striving to create a coherent framework that ensures data protection and promotes digital sovereignty. The key findings from the reviewed literature highlight several persistent themes:

- The need for harmonized and flexible regulatory frameworks that can adapt to rapid technological change while maintaining clear roles and responsibilities across different sectors and jurisdictions.
- The integration of ethical considerations into data security policies is crucial for building trust, promoting responsible AI deployment, and encouraging data sharing without compromising privacy.
- Emerging technologies like blockchain pose unique regulatory challenges that require innovative solutions balancing immutability with legal rights and compliance.
- Institutions like ENISA and legislative initiatives such as DORA are vital for coordinating cybersecurity efforts, but their success depends on overcoming political

resistance, capacity constraints, and tensions between national and supranational interests.

- The pursuit of digital sovereignty, especially in cloud computing, is a strategic priority that must balance the desire for control with the realities of economic competitiveness and global interdependence.
- Sector-specific approaches show that one-size-fits-all policies are ineffective; instead, tailored regulations that consider unique industry contexts and vulnerabilities yield better outcomes.
- External threats and geopolitical events significantly influence policy development, offering windows of opportunity for reform and highlighting the need for agile and responsive governance structures.

These challenges are further illustrated by Vilpisauskas (2024), who argues that despite the growing number of cyberattacks, political and institutional change was initially slow due to limited capacity, institutional fragmentation, and coordination problems.

Future research and policy development should continue to explore how these themes interact, striving for a more integrated, ethical, and resilient policy framework. Ongoing dialogue among EU institutions, member states, industry stakeholders, and academic researchers is essential to refine policies that can adapt to emerging challenges and fully realize the goals of data security, trust, and digital sovereignty in the European Union.

References

[1] Akgun, E. Z., Gerli, P., Mora, L., & McTigue, C. (2024). Breaking barriers for breaking ground: A categorisation of public sector challenges to smart city project implementation. PUBLIC POLICY AND ADMINISTRATION. https://doi.org/10.1177/09520767241263233

[2] Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernandez-Gutierrez, M. (2021). Blockchain for Public Services: A Systematic Literature Review. IEEE ACCESS, 9, 13904–13921. https://doi.org/10.1109/ACCESS.2021.3052019

[3] De Gramatica, M., Massacci, F., Shim, W., Tedeschi, A., & Williams, J. (2015). IT Interdependence and the Economic Fairness of Cybersecurity Regulations for Civil Aviation. IEEE SECURITY & PRIVACY, 13(5), 52–61. https://doi.org/10.1109/MSP.2015.98

[4] Blancato, F. G., & Carr, M. (2024). The trust deficit. EU bargaining for access and control over cloud infrastructures. JOURNAL OF EUROPEAN PUBLIC POLICY. https://doi.org/10.1080/13501763.2024.2441418

[5] Bygrave, L. A. (2022). Cyber Resilience versus Cybersecurity as Legal Aspiration. În T. Jancarkova, G. Visky, & I. Winther (Ed.), 2022 14TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: KEEP MOVING (CYCON) (pp. 27–43). IEEE; Microsoft; Fortinet; Meta; Singapore Univ Technol & Design, Ctr Res Cyber Secur; Thinklogical.

[6] Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. JOURNAL OF EUROPEAN PUBLIC POLICY, 31(8, SI), 2250–2286. https://doi.org/10.1080/13501763.2023.2295523

[7] Chiappetta, A., & Cuozzo, G. (2017). Critical Infrastructure Protection: Beyond the Hybrid Port and Airport Firmware Security Cybersecurity applications on transport. 2017 5TH IEEE INTERNATIONAL CONFERENCE ON MODELS AND

TECHNOLOGIES FOR INTELLIGENT TRANSPORTATION SYSTEMS (MT-ITS), 206–211.

[8] Donnelly, S., Camacho, E. R., & Heidebrecht, S. (2024). Digital sovereignty as control: The regulation of digital finance in the European union. JOURNAL OF EUROPEAN PUBLIC POLICY, 31(8, SI), 2226–2249. https://doi.org/10.1080/13501763.2023.2295520

[9] Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. JOURNAL OF EUROPEAN PUBLIC POLICY, 30(7, SI), 1330–1352. https://doi.org/10.1080/13501763.2023.2173274

[10] Koulas, E., Shah, S. I. H., & Peristeras, V. (2022). Webometric Network Analysis of Cybersecurity Cooperation. În K. Arai (Ed.), INTELLIGENT COMPUTING, VOL 1 (Vol. 506, pp. 103–122). https://doi.org/10.1007/978-3-031-10461-9_7

[11] Rone, J. (2024). `The sovereign cloud' in Europe: Diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. JOURNAL OF EUROPEAN PUBLIC POLICY, 31(8, SI), 2343–2369. https://doi.org/10.1080/13501763.2024.2348618

[12] Sivan-Sevilla, I. (2021). Europeanisation on demand: The EU cybersecurity certification regime between market integration and core state powers (1997-2019). JOURNAL OF PUBLIC POLICY, 41(3), 600–631. https://doi.org/10.1017/S0143814X20000173

[13] Sivan-Sevilla, I. (2023). Supranational security states for national security problems: Governing by rules & capacities in tech-driven security spaces. JOURNAL OF EUROPEAN PUBLIC POLICY, 30(7, SI), 1353–1378. https://doi.org/10.1080/13501763.2023.2172063

[14] Vilpisauskas, R. (2024). Gradually and then suddenly: The effects of Russia's attacks on the evolution of cybersecurity policy in Lithuania. POLICY STUDIES, 45(3–4, SI), 467–488. https://doi.org/10.1080/01442872.2024.2311155