European Commission

Joint Research Centre

SCIENCE FOR POLICY BRIEF – Digital Sovereignty Series

Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty

2025

HIGHLIGHTS

- As the first one in a series of policy briefs on Digital sovereignty, **this brief underscores that reducing Europe's critical dependencies will require the EU to consider targeted strategic actions in the field of digital sovereignty**. Our current and upcoming research is intended to help build the rationale for these actions by clarifying where interventions are most urgent to address critical vulnerabilities.
- EU digital sovereignty, **can be understood as the EU capacity to exercise strategic independence in the digital domain while remaining open and connected to global networks,** is essential for reducing vulnerabilities across economic, security, and technological spheres and for strengthening Europe's competitiveness. Despite major achievements in regulation and rights-based governance, the EU relies on non-EU providers for key technologies such as AI and cloud infrastructure, combined with structural limitations in independently managing and governing data.
- A holistic **multi-layered framework for digital sovereignty is proposed across four interlinked dimensions:** empowering people through rights and skills; fostering competitive and innovative digital markets; securing infrastructures, data, and software; and ensuring a governance that aligns regulation with legitimacy and global influence. It also calls for supporting research and development for key critical technologies that can foster Europe's digital sovereignty, particularly when competitive gaps exist with other geopolitical areas.
- **Building a realistic roadmap from ambition to implementation** requires science-for-policy research across multiple disciplines to guide prioritization and strategic action. These areas of inquiry (ranging from geopolitical exposure and technological dependencies to environmental impacts, legal enforcement and legitimacy, and social inclusion) highlight the broad societal, economic, and political implications of pursuing digital sovereignty and help clarify where its consequences are most significant.

1. Understanding EU Digital Sovereignty

In today's rapidly shifting geopolitical landscape, the EU faces an **urgent need to assert its digital sovereignty to safeguard democratic values, strengthen security, maintain economic competitiveness, and shape global standards**. This challenge unfolds on two fronts: a "today problem" and a "tomorrow problem."

The current predominance of non-EU ownership across key digital infrastructures already creates strategic vulnerabilities today, while simultaneously locking in trajectories that could entrench non-EU influence in future technologies and services, developments that may have even deeper and unpredictable consequences for European society and democratic governance (Mügge, 2024; Fratini, 2025).

Excessive reliance on non-EU technology providers coupled with the limited capacity to independently control and govern data, exposes vulnerabilities that could threaten EU democratic institutions and processes, compromise privacy protections and other fundamental rights, and weaken the resilience of critical infrastructures.

EU approach to digital sovereignty has evolved over time, shaped by enduring structural dependencies. Despite sustained regulatory and investment initiatives, the EU continues to depend on non-EU providers for key technologies such as design and production of semiconductors, cloud infrastructures, and Artificial Intelligence (AI), with implications for its strategic autonomy and capacity for innovation (Draghi, 2024). These dynamics point to the need for a shared and forward-looking understanding of EU digital sovereignty.

Digital sovereignty, however, **must not be conflated with isolation or protectionism**. In the European context, it can be described as the capacity of being independent while remaining open to collaboration and committed to shared values such as transparency, democracy, and the rule of law.

This policy brief is a first attempt to conceptualise EU sovereignty in the digital domain as the autonomous ability to manage and govern the EU digital stack -from data to AI, and the various digital technologies and services-, as well as to regulate, invest, and innovate within local and global networks, while preserving EU competitiveness and legitimacy in an increasingly contested international order (Leonard et al., 2019).

Unlike classical sovereignty rooted in territorial control, digital sovereignty should be exercised through the coordination of digital infrastructures, standards, software, and data governance (Floridi, 2020). Its effectiveness depends on the EU capacity to shape the frameworks—technological, regulatory, and institutional—through which digital systems operate. In this context, power appears increasingly distributed, yet in practice it is becoming more concentrated: private platforms and competing global powers act as de facto rule-makers, using their strategic advantages to reshape the boundaries of public-sector autonomy. The EU approach therefore requires a multi-layered strategy: empowering citizens and skills from the bottom up (legitimacy), fostering competitive markets and entrepreneurial capabilities (capacity), securing infrastructures and data ecosystems (resilience), and ensuring governance that projects European values without falling into protectionism.

Towards a Common Understanding of EU Digital Sovereignty

EU digital sovereignty is understood as the EU **capacity to exercise its independence in the digital domain while remaining open and connected to global networks**. It focuses on the ability to decide, invest, and innovate according to European values of democracy, openness, and the rule of law.

Rather than implying isolation or protectionism, digital sovereignty refers to **strengthening EU skills, infrastructures, and governance** to ensure that digital transformation supports competitiveness, resilience, and trust.

EU strength has historically lied in its regulatory and normative influence exemplified by the global reach of the GDPR, the Digital Services and Digital Markets Acts (DSA and DMA, respectively), and the AI Act (Bradford, 2020). Yet, this influence is no longer uncontested and is not sufficient alone to achieve digital sovereignty. Competing models—market-driven in the United States and state-centric in China—challenge the universality of EU rights-based vision (Farrand & Carrapico, 2022; Fratini et al., 2024). To remain credible, the EU must complement its regulatory power with industrial and technological capabilities, transforming sovereignty from a declarative ambition to a tangible capacity to act.

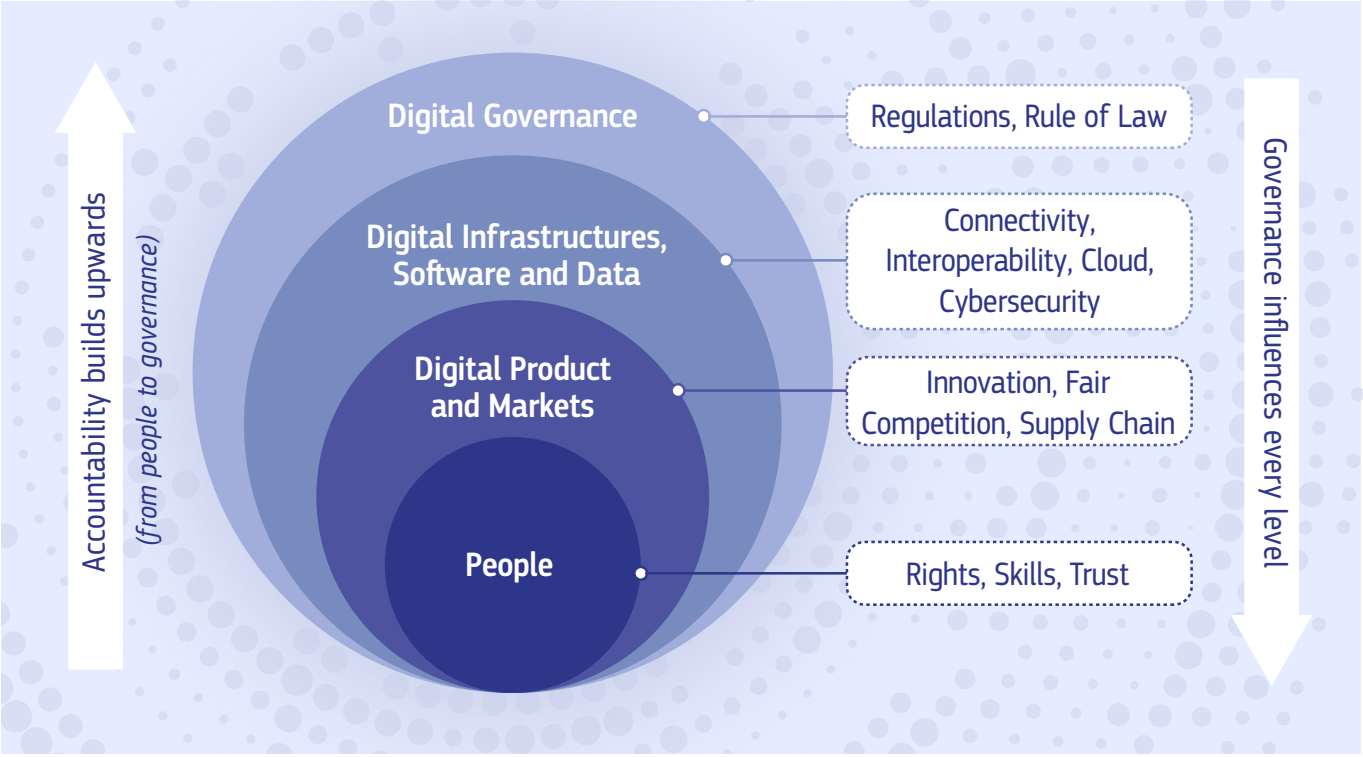
In a joint declaration, the EU27 Member States defines digital sovereignty as the "ability of "Member States" to act autonomously and to freely choose their own solutions, while reaping the benefits of collaboration with global partners, when possible" (Declaration for European Digital Sovereignty,

2025)[1]. This understanding, however, requires strengthening EU ability to decide and innovate by reducing strategic dependencies in critical technologies—semiconductors, cloud services, and AI—while embedding this autonomy within a framework of democratic accountability, trust, and fundamental rights (Monsees & Lambach, 2022). The distinctiveness of this approach lies precisely in the balance between autonomy and collaboration: rather than retreating from global cooperation, the EU seeks to shape it, aligning competitiveness and technological resilience with the protection of rights, fairness, and sustainability.

In this sense, **digital sovereignty in the European Union is understood as both practical and value-driven —anchored in shared rules and effective decision-making**. It should reflect the conviction that EU sovereignty in the digital domain cannot be achieved through isolation, but through the capacity to use and adopt digital technologies under its influence, guided by its values and interests.

Despite growing recognition of its importance, **the conceptualization and perceived vision of digital sovereignty continue to be fragmented across stakeholders and contexts** (Pohle & Thiel, 2020; Couture & Toupin, 2019) complicating efforts to establish cohesive policies and strategies that effectively address current and future EU vulnerabilities. To address this gap, this policy brief introduces a multi-layered framework for digital sovereignty with the objective of bringing together different perspectives, in a consistent and strategic manner (see Figure 1).

Figure 1. The Digital Sovereignty Framework: four layers shaping EU independence in the digital domain



Source: own elaboration.

The proposed framework works across four interconnected layers:

1. Digital Governance;
2. Digital Infrastructures, Software and Data;
3. Digital Products and Markets and
4. People.

By incorporating these multiple layers, the framework allows evaluating their various implications from a balanced perspective that acknowledges both the opportunities offered by EU strategic shift and the potential risks if sovereignty is pursued in a narrow or reductionist manner.

Moreover, the framework recognises a two-way relationship between accountability and governance: while sovereignty is built from the bottom up, governance decisions flow downward and shape every layer beneath them. Therefore, EU **digital sovereignty is not only a matter of technology or markets but also of legitimacy and democratic accountability**.

2. Digital Sovereignty implications

Based on the multi-layered framework introduced in the previous section, an overview of the key

implications associated with digital sovereignty is presented below. This overview examines the main opportunities and risks associated with each layer of the framework and helps identify areas where digital sovereignty can be strengthened, while also addressing potential vulnerabilities.

2.1 Digital Governance

Digital Governance constitutes the overarching layer, shaping the entire system through regulations, the rule of law, and policy coordination. Governance is not confined to formal institutions: it also determines EU ability to protect democratic values internally while projecting values internationally, balancing industrial and societal priorities, and ensuring that sovereignty does not become synonymous with protectionism. Moreover, effective digital governance plays a crucial role in upholding the integrity and transparency of EU democratic processes, facilitating a responsive and accountable system that reflects the collective interests of its Sember States and citizens in a rapidly evolving digital environment.

Opportunities. The EU has long been perceived as a regulatory power with its de facto global benchmarks. The Digital Service Act, the Digital Market Act, and the AI Act - building on the global influence of the GDPR - make the EU the first jurisdiction to codify a comprehensive, risk-based approach to platform and AI governance. At the multilateral level, EU has also sought to embed its rights-based model into frameworks such as the EU–US Trade and Technology Council, the OECD AI Principles, and the forthcoming UN Global Digital Compact.

Risks. Global governance is increasingly shaped by three competing models—European rights-based, US market-driven, and Chinese state-centric (Bradford, 2023)— and abroad the EU norms are at risk and no longer broadly adopted. At the same time, private firms increasingly act as rule-makers, embedding their own principles into platforms and infrastructures that shape user behaviour independently of legislation. If the EU does not act, there is a concrete risk that rules created and embedded by non-EU companies will end up determining how digital services operate within the Union. Moreover, the EU regulatory ambitions risk outpacing its industrial and technological capacity, creating a credibility gap between what the EU prescribes and what it can realistically enforced.

This evolving landscape suggests that the EU governance strategy can no longer rely solely on regulatory unilateralism. **Digital sovereignty at this level requires coalition-building, credible enforcement, and recognition of a multipolar governance arena,** where influence is negotiated rather than imposed.

2.2 Digital Infrastructures, Software, and Data

Digital Infrastructures, Software, and Data make up the backbone of digital sovereignty. This includes secure connectivity, interoperable systems, software and hardware, data ecosystems, cloud and edge infrastructures, and resilient cybersecurity. Control over data flows and security of infrastructures is vital to reduce vulnerabilities and protect both economic and democratic resilience.

Opportunities. EU has taken decisive steps to strengthen this layer. The *Digital Decade Policy Programme 2030* commits Member States to universal gigabit connectivity and 5G coverage across all populated areas (Decision (EU) 2022/2481, OJ L 323, p. 7)[2], making high-speed access a baseline right. For instance, the *EuroStack initiative* proposes a €300 billion, ten-year programme integrating cloud, AI Continent Action Plan and the establishment of AI Factories, and shared data commons into a federated European infrastructure (Bria, Timmers & Gernone, 2025, p. 4), positioning EU as a credible alternative to US and Chinese hyperscalers. Additionally, the *Open Source Software Strategy 2020-2023* promotes the sharing and reuse of software solutions to reinforce EU digital autonomy, while enhancing transparency and collaboration across borders.

Risks. Despite progress, structural vulnerabilities remain. ENISA's *Threat Landscape 2024* reported a 30% increase in ransomware attacks on EU critical infrastructures between 2022 and 2024 (p. 11), exposing weaknesses in cybersecurity coordination. Fragmentation is another risk: without stronger EU-level integration, national data-sharing projects may proliferate without interoperability, undercutting the promise of establishing a common European data space, as set out in the 2020 European Strategy for data.

Infrastructures and data ecosystems represent the most strategic layer of digital sovereignty: they are the foundation on which governance, markets, and individual rights depend. Yet digital sovereignty here is not only about ownership of infrastructures but also about the capacity to generate, store, process, and govern data in line with European values.

2.3 Digital Products and Markets

For Digital Products and Markets, digital sovereignty translates into the capacity to foster innovation, ensure fair competition, and prevent dependency on non-European providers. Competitive markets and a robust industrial base are crucial to sustain EU capacity to act independently.

Opportunities. By strengthening its capacity in strategic technologies, the EU aims to enhance resilience and geopolitical autonomy. Instruments such as the EU Chips Act—focused not only on boosting domestic production but also on diversifying and securing reliable supplier networks—and the forthcoming Cloud and AI Development Act that focuses on creating the right conditions to improve EU cloud capacity. Given the EU structural reliance on foreign semiconductor ecosystems, complete self-sufficiency is unrealistic; therefore, the Union must double down on diversification and strategic partnerships to safeguard its strategic autonomy while remaining open.

Risks. Structural vulnerabilities remain. EU accounts for only 7–8% of global AI R&D (OECD, 2023, p. 54). Cloud services remain dominated by non-European providers: over 90% of the EU market is controlled by US firms (European Commission, DMA monitoring, 2023, p. 7)[3]. On the one side, EU reliance on external markets for advanced semiconductors and critical raw materials, leave sovereignty susceptible to external shocks, supply chain disruptions, and geopolitical leverage. on the other side, excessive regulatory burdens risk falling disproportionately on SMEs and start-ups, reducing their ability to scale and compete.

The market layer underscores both the promise and fragility of EU industrial sovereignty. By mobilising regulation, investment, and innovation, the EU can strengthen its productive base and reduce critical dependencies. Yet without sufficient scale, integration, and industrial capacity, sovereignty risks becoming more rhetorical than real.

2.4 People (Citizens and Users)

People form the foundation of the framework, as digital sovereignty ultimately rests on the ability of individuals, communities, entrepreneurs, and other stakeholders to exercise their rights, build digital skills, and place trust in the technologies and institutions that govern the digital space. Without empowered and digitally literate citizens, sovereignty risks remaining a purely top-down project.

Opportunities. EU digital and data-related regulation (e.g., GDPR, DSA, DMA, Cyber Resilience Act and AI Act) illustrate how sovereignty can be translated into enforceable guarantees to fundamental rights, that distinguish EU values-based model from laissez-faire or state-centric approaches. This approach highly affects citizens as main users of digital public and private services and has the potential to empower agency from the bottom-up — for example, the *Digital Decade Policy Programme 2030* sets the target of 80% of adults with basic digital skills and 20 million ICT specialists by 2030 (Decision (EU) 2022/2481, OJ L 323, p. 15)[4].

Risks. Persistent gaps in skills and trust threaten legitimacy. According to the DESI 2024, only 55.6% of Europeans had basic digital skills as of 2023 (European Commission, 2024, p. 16). Eurobarometer 551 shows that just 45% of citizens believe the EU protects their rights online (p. 21). If digital sovereignty is perceived as technocratic or exclusionary, it risks undermining the very trust on which EU autonomy depends.

The people layer reveals that rights-based regulation and ambitious skill targets can empower citizens as active participants in EU digital future. Yet persistent divides in literacy, access, and confidence risk turning digital sovereignty into a project *about* people rather than *for* them.

3. Policy considerations

The research shows that, although digital sovereignty is gaining prominence as a key EU priority, it still lacks a clear, shared definition and a coherent approach to implementation. The challenge for the EU is therefore twofold: first, the need in advancing conceptual and empirical understanding of sovereignty as a multi-layered concept; and second, the necessity in translating this understanding into policy instruments that balance external dependency with continued competitiveness, and democratic accountability.

From a governance perspective, the EU regulatory capacity remains its most distinctive expression of sovereignty, yet its effectiveness depends on the capacity to evolve with shifting technological and geopolitical dynamics – condition that cannot be assumed in an increasingly plural and contested digital order. **Digital sovereignty today requires a form of regulatory adaptability that is both internally coherent and externally credible.** This implies aligning diverse policy domains under a shared strategic vision capable of reconciling openness with autonomy.

Fragmentation across institutional levels, and inconsistencies between internal and external policy objectives, have often diluted the EU influence in multilateral settings. Coherence, therefore, becomes not merely a procedural matter but a substantive condition for sovereignty: the ability to act collectively, articulate shared priorities, and sustain legitimacy in global digital governance debates. Building such coherence may depend less on asserting control and more on fostering interdependence on equitable terms, through

frameworks that emphasize accountability and democratic oversight across digital ecosystems.

Infrastructural and data-related dimensions of sovereignty reveal equally persistent challenges, calling for clearer prioritization and coordinated investment. Bottlenecks in connectivity, cybersecurity, and data management continue to constrain strategic autonomy. The gradual implementation of initiatives such as EuroStack, along with the operationalisation of the Critical Raw Materials Act through diversification and strategic stockpiling, may help mitigate vulnerabilities. At the same time, progress toward interoperable and trusted sectoral data spaces (for example, in health, mobility, energy, and manufacturing) could translate high-level ambitions into concrete outcomes. Dependence on non-European technical solutions remains a strategic concern comparable to reliance on imported materials or technologies. Addressing fragmentation among national initiatives will be critical, as effective sovereignty depends less on duplication and more on federation, interoperability, and shared governance.

Industrial and market dimensions form another pillar of EU sovereignty. The Union's experience with industrial policy has been mixed: while initiatives such as the EU Chips Act demonstrate ambition, they also underscore the risk of fragmentation between national priorities. Ensuring effective governance and coordination will be as important as securing financial resources. **The role of small and medium-sized enterprises is particularly salient in this context.** Without proportionate regulatory approaches, there is a risk that compliance burdens designed for large corporations could constrain smaller innovators who are essential to Europe's technological resilience and diversity.

Finally, **digital sovereignty derives much of its legitimacy from societal inclusion and trust.** Bridging Europe's digital skills gap requires not only education reform but also long-term investment in lifelong learning, reskilling, and inclusion programmes that reach disadvantaged groups. Rights-based frameworks such as the GDPR, DSA, DMA, and AI Act become meaningful when citizens can see their tangible effects, whether through transparent data practices, accessible redress mechanisms, or visible accountability in algorithmic systems.

Building a realistic and adaptive **roadmap for digital sovereignty ultimately depends on the EU ability to prioritize,** systematically documenting initiatives, evaluating their impacts, and drawing lessons from both successes and failures. Regulatory milestones such as the GDPR's global influence demonstrate the EU potential to shape digital governance, while persistent dependencies in cloud and cybersecurity reveal the limits of current approaches (Bellanova et al.,2022). Learning from this dual experience is essential if sovereignty is to evolve as a dynamic, evidence-based process rather than remain an aspirational policy objective.

4. Emerging Science for Policy Research Agenda

Digital sovereignty emerges as a multi-layered and evolving issue, situated at the **intersection of geopolitical exposure, environmental constraints, legal and governance capacity, technological interdependence, and social inclusion**.

These di-mensions are not discrete policy fields but **complex, interdependent domains,** each marked by overlapping vulnerabilities. Science for policy can contribute by clarifying how sovereignty is enacted and measured across these domains, not to converge on a single model but to map the diverse pathways through which digital sovereignty is contested and coconstructed in practice. Within this broader landscape, two topics emerge as particularly consequential: innovation and procurement. While they do not exhaust the debate, they represent the most tangible levers through which digital sovereignty is negotiated today. We will examine both domains in greater depth in future briefs of this series.

The **geopolitical dimension** highlights that the EU operates within an open and interdependent system shaped by supply chain shocks, standardization rivalries, and regulatory competition. To foster digital sovereignty, it is crucial to understand when and how EU norms extend beyond its borders and when they remain bounded by institutional, market, or technological limitations. Comparative analysis of global innovation and governance models can shed light on how different configurations of public, private, research actors and civil society gener-ate strategic leverage. Science for policy work could help to better understand systemic exposures, such as the effect of disruptions in semiconductor supply chain or restrictions on cross-border data flows and explore how technological open-ness and autonomy can be balanced through adaptive design rather than isolation.

The **environmental dimension** shows that digital sovereignty is materially and energetically constrained. Without adequate energy and material infrastructures, data governance and storage remain incomplete and structurally vulnerable. Understanding how frameworks such as the Critical Raw Materials Act are implemented in practice,

including diversification mechanisms and stockpiling strategies, is therefore essential. At the same time, frontier research on energy-efficient computing, circular hardware systems, and low-impact data infrastructures is crucial to reframing sustainability not as a parallel objective but as a foundation for sovereignty. The environmental footprint of digital infrastructures represents a structural bottleneck that directly affects strategic resilience. In this regard, it is worth recalling that digital sovereignty must align with the EU's net-zero commitments and climate targets, ensuring that strategic choices in the digital domain reinforce—rather than undermine—Europe's long-term decarbonisation pathway.

The **legal dimension** reflects the EU distinctive as-set, regulatory power, but also its inherent limits. The so-called Brussels Effect represents an empirical dynamic of influence, not a structural constant. Regulatory strength depends on implemen-tation, adaptability, and credibility. Future research could examine how experimental instruments such as sandboxes, algorithmic audits, or regulatory technologies influence compliance and trust. It could also investigate how rights-based frameworks become socially meaningful, focusing on whether citizens experience data protection, algorithmic transparency, and accountability in every-day digital interactions rather than solely through legal provisions. Here, possible role of public institu-tions might deserve special attention, for example, to understand how public administrations can be inclusive and open, while supporting autonomy (Millard, 2023).

Regarding the **technological dependency dimension**, evidence from past initiatives, including delays, uneven adoption, and fragmented strategies, indicates that cloud, data, semiconductors, and cybersecurity show that those systems are interdependent rather than separate domains. Sovereignty in this field depends on federation through shared governance, interoperability, openness, and coordi-nated implementation rather than replication. Science for policy can contribute by developing concrete methodologies such as resilience metrics, interdependencies measures among different technological areas and sectors, dependency ratios, interoperability benchmarks, and recovery-time indicators that make progress measurable and comparable.

The **social dimension** reminds us of that sovereignty ultimately depends on collective capacity. It relies on citizens, entrepreneurs, and workers who can not only use but also understand and shape digital systems. Current assessment frameworks—exemplified by robust models such as DigiComp 3.0—are beginning to incorporate emerging digital competencies, but digital sovereignty remains largely absent from citizens' competency profiles and public awareness, reflecting its still-emerging role in the digital governance landscape. This absence points to the need for deeper empirical inquiry into how citizens conceptualize democracy and inclusiveness within an environment increasingly shaped by digital platforms and social media. Cross-national research could further illuminate how citizens in different Member States make sense of digital sovereignty and how its associated advantages and burdens are distributed across communities, regions, and socio-economic groups.

Across these five interdependent domains, the next step for the science-for-policy community is to **connect diverse strands of evidence into a coherent measurement framework**. The aim is not to multiply indicators but to strengthen the capacity to observe sovereignty as a moving target. This includes assessing whether exposure to vulnerabili-ties is decreasing, whether autonomy is substantively expanding, whether infrastructures are becoming more federated, and whether rights and skills are reflected in the lived experience of European citizens. Such an evidence base would allow policymakers and researchers to reveal where progress is occurring and where gaps persist. As part of this effort, we will also **carry out a thorough dependency analysis to understand the true scale of the issue,** recognising that the most critical element is the price tag of sovereignty, which represents the main constraint on implementing it. This is the first policy brief in a series designed to explore these different but systemically related domains in greater depth. Building on various the-matic clusters, each brief will translate research findings into targeted policy insights and identify emerging evidence needs.

-

1 Retrievable at: Note from the Council of the European Union (General Secretariat) to EU Member State delegations (ST-15781/25 (TREE2B EN) pdf

2 Retrievable at: Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance) Decision - 2022/2481 - EN - EUR-Lex

3 Retrivable at: REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Annual report on Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) EUR-Lex - 52024DC0106 - EN - EUR-Lex

4 Retrievable at: Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance) Decision - 2022/2481 - EN - EUR-Lex

References

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. European Security, 31(3), 337–355.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world.* Oxford University Press.

Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack–A European alternative for digital sovereignty.

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322.

Draghi, M. (2024). "The future of European competitiveness part A: A competitiveness strategy for EU." (2024).

Farrand, B., & Carrapico, H. (2022). Digital Sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. European Security, 31(3), 435–453.

Floridi, L. (2020). 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU'. Philosophy & Technology 33 (3): 369–78. https://doi.org/10.1007/s13347-020-00423-6

Fratini, S. (2025). The sociotechnical politics of digital sovereignty: Frictional infrastructures and the alignment of privacy and geopolitics. Big Data & Society, 12(4),https://doi.org/10.1177/20539517251400729

Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society, 3(59).

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8(1).

Ilves, L., & Osula, A.-M. (2020). The technological sovereignty dilemma – and how new technology can offer a way out. European Cybersecurity Journal, 6(1), 24–33.

Ivic, S. and Troitiño, D.R., (2022). Digital Sovereignty and identity in the European union: A challenge for building EU. European Studies, 9(2), pp.80-109.

Leonard, M., Pisani-Ferry, J., Ribakova, E., Shapiro, J., & Wolff, G. B. (2019). *Redefining Europe's economic sovereignty* (Vol. 9). Brussels: Bruegel.

Millard, J. (2023). Impact of digital transformation on public governance. *European Union, Luxemburg.*

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security, 31*(3), 377-394.

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? Journal of European Public Policy, 31(8), 2200–2225.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review,* 9(4).

Acknowledgements

We extend our gratitude to the time and expert feedback offered by Julia Pohle, Anna Colom, Samuele Fratini, Gianluca Sgueo, George Breyiannis, Manlio Bacco, Brooke Tapsall, Andrea Ceglia, Michele Vespe, Sven Schade, Romina Cachia, Giuditta de Prato, Elena Navajas Cawood, Roberto Ugolotti, Gianmarco Baldini, Erica di Girolamo, Project Leaders of JRC Unit T1 and Head of Units of all JRC Dir T that have improved the quality and effectiveness of this policy brief. We thank Raffaella Manfredi for her contribution to the graphical design of this policy brief.

Suggested citation

How to cite this report: Di Marco D., Thabit S., Kotsev A., Christensen A., Minghini M. et al., *Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty*, European Commission Ispra, 2025, JRC144908.

Disclaimer

The opinions expressed are those of the author(s) only and should not be considered as representative of the Joint Research Centre's official position.

Copyrights

Science for policy

Scan the QR code to visit:
The Joint Research Centre: EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC144908

CONTACT INFORMATION

European Commission — Joint Research Centre (JRC)
Contact: Alexander Kotsev
E-mail: Alexander.KOTSEV@ec.europa.eu