IPC–MERCATOR ANALYSIS

October 2026

DIGITAL GEOPOLITICS AND SOVEREIGNTY: CONVERGENCE AND DIVERGENCE BETWEEN THE EU AND TURKEY

Jacopo Franceschini



IPC

ISTANBUL POLICY CENTER
SABANCI UNIVERSITY
STIFTUNG MERCATOR INITIATIVE

Introduction

Within the space of nine weeks in the spring of 2026, Ankara and Brussels each practiced digital sovereignty in its own idiom. On April 1, Turkey launched its commercial 5G network. This followed a tender held on October 16, 2025, in which the government attached domestic content requirements of up to 60% for the new network.[1] On June 3, the European Commission followed with its Tech Sovereignty package, comprising a Chips Act 2.0, a Cloud and AI Development Act, and an open-source strategy, presented as a major shift in the EU's approach to technology.[2]

Both acts were carried out in the name of digital sovereignty: both highlight its central paradox. The EU is still dependent on suppliers outside its borders for more than 80% of its key digital products, services, infrastructure, and intellectual property.[3] Turkey's new networks will run, at least in part, on foreign vendors' equipment. Despite both actors' push for digital sovereignty, neither actor can be sovereign alone.

Against this backdrop, this analysis asks what digital sovereignty actually is, over what objects it is claimed, why it has become central to geopolitics and international relations, how the European Union and Turkey each construct it, where the two constructions clash or prove compatible, and what each side would gain from a convergent approach. The analysis argues that the EU and Turkey have two different definitions of digital sovereignty, one normative and one technological. However, both share adversaries, threat framings, and an unspoken assumption that full autonomy is impossible. Precisely because sovereignty in the digital domain can only be exercised through relationships, a convergent approach is not a dilution of sovereignty but its most realistic form.

What Is Digital Sovereignty and Over What Objects Is It Claimed?

The concept of digital sovereignty did not originate in Brussels but in autocratic contexts. Russia and China first articulated notions of internet or cyber sovereignty to shield domestic networks from outside interference.[4] The scholarly genealogy of the concept traces its roots to early contestation of American dominance over digital infrastructure and their governance.[5] Edward Snowden's revelations of American government surveillance in 2013 then carried the debate into European democracies. A French Senate report warned as early as 2013 that Europe risked becoming a colony of the digital world, and by 2020, Germany's EU Council Presidency had elevated digital sovereignty to become a guiding motif for European digital policy.[6]

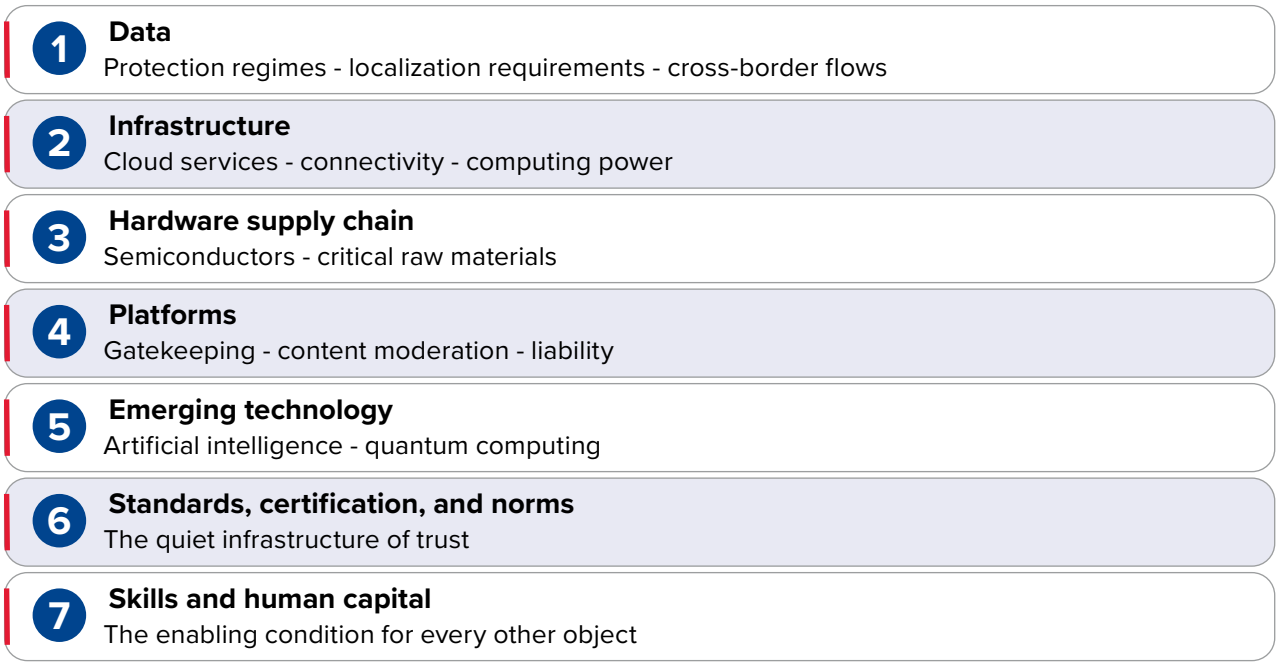
In official usage, the concept denotes a capacity: defined by the European Commission as "the capacity to act independently in the digital domain, resting on the development and control of key technologies, data, and infrastructure and on reduced reliance on providers outside the EU."[7] Scholars, in contrast, increasingly treat digital sovereignty not as an objective status but as a claim, a discursive resource deployed in political struggles over the control of digital networks, whose meaning shifts depending on the actor calling for it.[8] Recent conceptual work identifies five recurring attributes of such claims. They are adversarial, since they are always directed against someone; multiverse, since they justify multiple and even contradictory policy directions; latent, since they are asserted or withheld strategically; instrumental, since they are attached to concrete policy dossiers; and marked by a structural gap between rhetoric and practice.[9] A further analytical distinction identifies three types of claims: those concerning state autonomy and the security of national infrastructure, those

concerning economic autonomy vis-à-vis foreign technology providers, and those concerning the digital self-determination of individual users.[10]

Over what, concretely, is digital sovereignty claimed? Its objects have multiplied as sovereignty claims have been extended across every layer of the digital space.[11] Seven stand out (Figure 1). The first is data, covering protection regimes, localization requirements, and cross-border flows. The second is infrastructure, from cloud services to connectivity and computing power. The third is the hardware supply chain, including semiconductors and the critical raw materials behind them. The fourth is the platform layer, where gatekeeping, moderation, and liability are decided. The fifth is emerging technology, above all artificial intelligence and quantum computing. The sixth is the quiet infrastructure of trust made of standards, certification, and norms. The seventh is skills and human capital, without which every other object remains notional. Each object generates its own politics, its own dependencies, and its own instruments.

Every one of these claims, however, eventually collides with the material reality of interdependence. Digital sovereignty rests on a paradox, promising autonomy in a domain in which the European Union, Turkey, and indeed every state depend on others for critical layers of their digital stack.[12] Semiconductors illustrate this point, since no single actor controls the full value chain.[13] Sovereignty has, in this sense, always been a form of "organized hypocrisy," and its digital variant is no exception.[14] The practical consequence is that the concept is best studied through what is done in its name, through the budgets, subsidies, and laws it legitimizes, rather than as a coherent doctrine. Part of its political utility lies precisely in its capacity to justify heterogeneous initiatives without explaining how they cohere.[15]

Figure 1. The Seven Objects of Digital Sovereignty



Source: Author's elaboration.

The Geopolitical Stakes

If digital sovereignty has become part of the lingua franca of international politics, it is because technology has moved to the heart of great power rivalry. Technological capacity now functions as a condition of international ascent rather than a mere driver of growth,[16] and the networked structure of the digital economy allows states that control its choke points to weaponize interdependence, converting supply chains, payment systems, and data flows into instruments of coercion.[17] The rivalry between Washington and Beijing constrains all other actors, since the governance of the digital ecosystem, from standards to infrastructure to platforms, is largely concentrated in their hands. All other states must position themselves in relation to those poles.

Sovereignty claims are made against someone. To assert authority over data, infrastructure, or platforms is to contest the control that another actor, a foreign state, a firm, a standards body, currently exercises; it is in this sense that such claims are adversarial. Through this reading, the map of digital sovereignty discourse is a map of conflict. Regime type, notably, does not predict the discourse—for in adversarial terms, the EU's claims resemble those advanced by China and Russia, while the United States began speaking the language of sovereignty only once Chinese technology challenged sectors it had long dominated.[18] This adversarial logic reaches into Europe even where Europe holds the asset. In semiconductors, a single Dutch firm holds a near-monopoly over one stage of advanced chipmaking, and yet it has followed Washington's instructions rather than any European strategy in its export decisions. The choke point is European; the strategy governing it is not.[19] The stakes do not depend on hostile intent, however. The global outage of CrowdStrike software in July 2024, triggered by a faulty update rather than an attack, grounded aircraft and disrupted hospitals across continents; the same interdependence that rivals can weaponize can also simply fail.[20]

Beyond discourse, the concept moves money on a scale that is reason enough to take it seriously. The European Union's Chips Act is meant to mobilize some EUR 43 billion in public and private investment, the Global Gateway carries a EUR 300 billion budget for 2021–2027, and the raw materials agenda sets supply benchmarks for 2030; all three are justified in the name of sovereignty. The tempo has accelerated since the 2024 Draghi report on European competitiveness, which tied the EU's economic prospects to its technological dependencies and put the additional investment Europe needs at roughly EUR 750–800 billion a year.[21] A Declaration for European Digital Sovereignty, initiated by Austria, was adopted by the EU member states in the run-up to the Franco–German Summit on European Digital Sovereignty held in Berlin in November 2025. The Commission's Cloud Sovereignty Framework of October 2025 now translates the concept into procurement criteria, and the Commission's European Technological Sovereignty Package of June 2026 followed, proposing a Chips Act 2.0 and a Cloud and AI Development Act that would introduce an EU-wide framework for assessing the sovereignty of cloud and AI services.[22]

For the small and semi-peripheral states in and around the EU, the newer member states of Central and Eastern Europe and the candidate countries on its edges, digital sovereignty has different implications. Most such states are simultaneously small and dependent, a dual disadvantage that shapes how they adopt and adapt the agenda.[23] The concept can also be bent to local political ends, since, for example, in Hungary, restrictive

content moderation has been justified in the name of digital sovereignty; in Latvia, the discourse has taken a militarized, anti-Russian inflection. For a large candidate country such as Turkey, the question is starker still: should it become a rule-taker inside someone else's technology ecosystem or negotiate the terms of interdependence?

The EU Approach: Sovereignty through Rules

Between 2019 and 2026, European anxiety about technological dependence hardened into architecture. The 2019 political guidelines of the incoming Commission declared it "not too late to achieve technological sovereignty in some critical technology areas."[24] In 2020, the President of the European Council framed technological independence as the capacity to make the EU's own choices, reduce dependencies, and defend European interests and values.[25] The claim was layered onto an already dense regulatory stack, each layer of which governs a different part of the digital economy: personal data under the General Data Protection Regulation (GDPR), online platforms and gatekeepers under the Digital Markets and Digital Services Acts, artificial intelligence under the AI Act, and the security of networks, connected products, and financial systems under the revised Network and Information Security Directive (NIS2), the Cyber Resilience Act, and the Digital Operational Resilience Act (DORA).[26] These instruments made the EU the principal rule-setter of the digital economy but did not change where its technology is produced. Thus, an industrial arm was added to address that gap: the Chips Act to expand semiconductor manufacturing in Europe, the Gaia-X initiative to build a federated European cloud, and the Digital Decade targets to set 2030 goals for skills, infrastructure, and the digitalization of business and government. Since 2024, a competitiveness turn has pulled the agenda in two directions at once. The Digital Omnibus, whose AI component was adopted in June 2026, defers the AI Act's high-risk regime, the Act's strictest tier of obligations reserved for AI used in sensitive areas such as hiring, credit, education, critical infrastructure, and law enforcement, Under Regulation (EU) 2024/1689. "High-risk" AI systems are those used in listed sensitive areas (biometrics, critical infrastructure, education, employment, access to essential services, law enforcement, migration, and the administration of justice) or as safety components of products covered by EU product legislation. Their providers must comply with the Act's core requirements (risk management, data governance, technical documentation, human oversight, accuracy, and cybersecurity) and undergo a conformity assessment before placing them on the market. The Omnibus postpones these obligations to December 2027 for stand-alone systems and to August 2028 for product-embedded systems, while leaving most transparency obligations to apply from August 2026.[27] It also tightens control over supply: a January 2026 cybersecurity package converts the voluntary logic of the 5G security toolbox into a binding framework for supply-chain risk, and the Tech Sovereignty Package of June 2026 proposes a Chips Act 2.0 and a Cloud and AI Development Act.[28]

What emerges from this architecture is less a doctrine than a pattern in practice through an EU model of digital sovereignty that can be described as sovereignty through rules. Rather than pursuing improbable self-sufficiency in production, the EU seeks security and reduced dependencies through law, standards, certification, and targeted investment, counting on the extraterritorial pull of its single market to carry its frameworks

abroad.[29] Analysts have characterized the trend as a progressive fusion of security and regulation, in which security objectives are pursued through regulatory instruments, and regulation is in turn justified on security grounds.[30] Some describe this trend as an increasingly assertive, even mercantilist, use of regulatory power in the digital domain.[31]

In its official presentation, the EU model is value-driven, centered on fundamental rights, democracy, and a human-centric digital transformation. Beneath the discussion of "protecting values," however, lies a more geopolitical subtext. The language of rights often encodes China as a threat to the EU's digital sovereignty. However, the platform rulebook points in the opposite direction, since nearly all the gatekeepers designated under the Digital Markets Act are American companies, and the EU's most muscular regulatory instruments in practice discipline the firms of its principal ally.[32] Chinese equipment in networks, American dominance of platforms and the cloud, and Russian disinformation give the EU's sovereignty claim three directions at once.

None of this means that rules deliver sovereignty on their own, and the limits of the EU model are well documented. Gaia-X, launched to build a European cloud independent of the American hyperscalers, admitted that it was using software from Microsoft and Amazon within roughly a year of its creation.[33] The dispute between regulation and innovation, meanwhile, remains unresolved. A familiar quip holds that Americans innovate, Chinese emulate, and Europeans regulate. Yet even the 2024 Draghi report, the sharpest critique the EU has faced in a decade, stops well short of recommending that the EU deregulate in order to spark innovation.[34] The June 2026 amendments point the same way, adjusting the AI Act's timetable without dismantling its framework.[35]

Turkey's Approach: Sovereignty through Capacity

Turkey describes digital sovereignty as a technological issue and, at times, an existential one. Its master framework is the National Technology Initiative (*Milli Teknoloji Hamlesi*), a holistic development vision aimed at a fully independent high-tech Turkey,[36] a goal reaffirmed by the Minister of Industry and Technology in 2026.[37] Comparative observations suggest that national approaches to digital sovereignty vary widely and that three patterns recur: a reactive sovereignty that responds to dependence on foreign suppliers by cultivating domestic industry, an identity-based sovereignty in which technology becomes part of what the nation is, and a pragmatic sovereignty of diversification, balancing, and selective engagement.[38] Turkey combines all three. The identity-based pattern is unmistakable in presidential rhetoric tying full political independence to technological independence, in the TEKNOFEST festivals staging technology as national pride, and in the official doctrine of a cyber homeland (*siber vatan*), to be defended like land, sea, and air.[39] Treating cyberspace as a domain of defense is not in itself distinctive, since NATO, of which Turkey is a member, has recognized it as an operational domain since 2016,[40] and many EU member states have built military cyber commands on that basis. What is distinctive is the idiom of homeland, which makes cyberspace an extension of national territory and identity rather than merely a theater of operations. It is precisely this fusion of technology with national identity that sets Turkey's approach apart.

Since 2024, reactive sovereignty— the response to dependence on foreign suppliers, now framed as a security threat— has hardened into strategy, decree, and statute. A new National Cyberse-

curity Strategy and Action Plan for 2024–2028, prepared by the Ministry of Transport and Infrastructure, was put into effect by Presidential Circular 2024/11 of September 2024,[41] followed by two further steps. Presidential Decree No. 177 of January 2025 created the Cybersecurity Directorate (*Siber Güvenlik Başkanlığı*), a body with its own budget attached directly to the Presidency.[42] The Cybersecurity Law of March 2025 provided the country's first comprehensive legislation in the field, defining cybersecurity as an integral part of national security, creating a Cybersecurity Board chaired by the president and writing a statutory preference for domestic components into law.[43] Another decree in March 2025 then closed the Digital Transformation Office and moved its functions, from e-government services to public-sector artificial intelligence, into the aforementioned Cybersecurity Directorate. The new directorate's mandate expanded beyond cybersecurity to include the digital realm as a whole after a December 2025 decree, while a law adopted by parliament on July 24, 2026, (Law No. 7590) transferred to the same body the telecommunications regulator's powers over domain names, internet infrastructure, and the detection and analysis of communications, including its role in access-blocking procedures under the Internet Law. The law authorized the directorate to order measures directly in urgent cases, even as the law's implementing regulations have yet to be finalized.[44] The replacement of an office for digital transformation by a body created by presidential decree for cybersecurity, and the transfer to that body of powers once held by the telecommunications regulator, can be read as signals of centralization and securitization in digital governance: e-government and public-sector artificial intelligence now sit under a security authority. The rationale that runs through all these measures is a single threat perception. Imported cybersecurity products are treated as a potential backdoor into critical infrastructure; domestic components therefore become a matter of national security rather than of industrial policy, and cybersecurity a matter for the presidency itself. This is reactive sovereignty in statutory form.

Alongside Turkey's drive toward the indigenization of its digital infrastructure, however, runs a deliberate layer of European alignment. Turkey's personal data protection law was modeled on EU law, and its 2024 amendment rebuilt its cross-border transfer regime, including its adequacy decisions, standard contractual clauses, and binding corporate rules, based on the architecture of the GDPR.[45] Turkey has taken part in the Digital Europe Programme as an associate country since 2023, under an agreement that, as for other associate countries such as Serbia and Ukraine, excludes the program's cybersecurity objective.[46] Several artificial intelligence bills are pending in parliament, including a draft law inspired by the EU's AI Act.[47] Additionally, the parliamentary AI Research Commission, whose roughly 900-page report was presented in February 2026, recommends, among other things, that Turkey consider signing the Council of Europe Framework Convention on artificial intelligence.[48] Turkey's digital state capacity is meanwhile genuinely impressive, with the e-Devlet gateway counting 68.2 million registered users and more than 9,100 services by the end of 2025, a level of digitized service delivery that compares favorably with much of Western Europe, although the infrastructure remains, for now, not interoperable with that of the EU.[49] Independent Turkish analysts also largely support Turkey's alignment and interoperability with European cybersecurity frameworks.[50]

Taken together, Turkey has built a model of sovereignty through adapting and owning technology capacities and regulations rather than defining

them. The model's internal tension is most visible in artificial intelligence, where the same parliamentary report that recommends a national AI security strategy to be prepared under the Cybersecurity Directorate, the defense industry agency, the armed forces, and the intelligence services also urges consideration of the Council of Europe Framework Convention.[51] Externally, in contrast, pragmatism prevails, as hard sovereignty language at home coexists with NATO cyber principles and exercises, participation in international incident-response networks, confidence-building at the OSCE, and an emergent technology diplomacy, consistent with Turkey's broader tradition of strategic autonomy.[52] What Turkey still lacks is a framework for integration. The number of instruments increases—the National Technology Initiative, the cybersecurity strategy, a national AI strategy, the digital chapter of the five-year development plan—but nothing ties them to a single set of measurable goals. The EU's Digital Decade program is the relevant comparator not because Turkey should copy it but because of the function it performs: it sets 2030 targets for skills, infrastructure, business, and public services, requires national roadmaps, and reports annually on progress, so that the acts and funds described in the previous section are steered and measured against common objectives. It is that integrating function, not any particular target, that has no Turkish equivalent.[53]

Divergence and Compatibility

The first point of divergence between the European and Turkish approaches lies in their philosophy of control. The EU regulates what it cannot build, while Turkey builds what it cannot regulate, and their referent objects differ accordingly. What the EU's rules set out to protect is not only infrastructure and data but a set of values such as fundamental rights, democracy, and an open, stable, and secure global internet.[54] What the Turkish framework protects is, first of all, the security of the state: the 2025 law anchors cybersecurity squarely within the field of national security, defining it as an integral part of state security.[55] Institutional temporalities differ as well—with the EU procedural, supranational, and comparatively slow, while Turkey's centralized governance can legislate and reorganize quickly, a difference that cuts both ways for cooperation.

A second point of divergence is relational, since the relationship is asymmetric and short on trust. Turkey aligns largely as a rule-taker rather than a rule-maker within a Customs Union that renders a measure of alignment effectively compulsory.[56] The trust deficit concentrates precisely where sovereignty claims are the strongest. Turkey's association with the Digital Europe Programme excludes the cybersecurity objective,[57] and the Commission's Türkiye 2025 Report assesses the country as having only "some level of preparation" on digital transformation and media while warning that the new cybersecurity law contains vague rules and lacks independent oversight.[58] Beneath similar texts, governance philosophies diverge, as Turkey sits uneasily between the rights-based and the state-control archetypes of digital governance, and textual convergence does not by itself change governance culture, producing alignment on paper.

The gap is widest where digital sovereignty meets freedom of expression. Turkey requires platforms to appoint local representatives and has built an extensive content-regulation practice, but it has no equivalent of the Digital Services Act, and its approach to online content owes more to state control than to procedural rights. For Brussels, where platform rules are welded to fundamental-

rights safeguards, this is not a technical detail, because it conditions how far data can flow, how much intelligence can be shared, and whether an adequacy decision is conceivable. The layer of digital sovereignty concerned with the self-determination of users is precisely the layer on which the two approaches remain furthest apart.[59]

Setting aside these divergences, however, the frameworks are largely compatible. The compatibility begins with position rather than with rhetoric: both actors depend on external technology providers and large platforms that they do not control but define their sovereignty against that dependence, and both hedge between Washington and Beijing so that their sovereignty claims are aimed at the same set of outside actors.[60] Their threat framings converge as well, since both sides now treat cybersecurity as a matter of core national security and infrastructural resilience rather than of technical housekeeping.[61] The legal layers already touch, since the data protection regimes mirror one another. Turkey's 2025 cybersecurity law inhabits the same conceptual world as the EU's NIS2 Directive, and the draft AI law before parliament takes its architecture from the EU's AI Act rather than from American or Chinese models: it classifies systems by risk, requires registration and conformity assessment for high-risk uses, and enforces this with turnover-based fines. However, the bill is far thinner than its model. In eight articles it leaves the definition of "high-risk" undefined, states providers' obligations only as general principles, and names no supervisory authority, leaving the details to secondary legislation.[62] The economies are complementary, with Turkey among the EU's leading high-technology export markets in 2023, accounting for EUR 14 billion in EU high-tech exports, EUR 362 million received by Turkish entities from EU research programs since 2003, and a young talent pool that could help meet a European shortage of digital skills.[63] The deepest connection of all is a shared and rarely spoken premise, namely that neither side actually pursues autarky. The drift of EU discourse toward ecosystems and resilience amounts to a tacit admission that cooperation, including with rivals, is unavoidable.[64] Turkey states the same in its own idiom since the 2024–2028 cybersecurity strategy lists international cooperation among its priorities, the national AI strategy sets harmonization with international standards as an objective, Ankara has kept its association with Horizon Europe and the Digital Europe Programme, and it is building its networks with European and Chinese vendors side by side.

The present state of play is best described as "structural convergence without relational cooperation."[65] The texts converge while the institutions, oversight, and trust do not. That gap, relational rather than textual, is where a convergent approach must operate.

The Benefits of a Convergent Approach

Properly understood, convergence between the EU's and Turkey's digital policies is neither doctrinal uniformity nor a rerun of accession conditionality but managed interdependence: that is, operational alignment on skills, standards, and procedures in areas where interests converge and risks are shared, without any requirement of identical sovereignty doctrines.

For the EU, the gains begin with scale, since a neighboring market of 85 million applying compatible rules extends the reach of European standards beyond the EU's borders and gives its regulatory model the weight that its competitiveness agenda demands.[66] Nearshored, standards-compatible

supply chains diversify dependencies that the EU's June 2026 Tech Sovereignty package can only partially address, while Turkey's talent pool could relieve a structural skills shortage. A further gain is strategic denial. Turkey is building out its networks now, and European and Chinese vendors are both in the running. If Brussels disengages, it risks pushing Ankara toward the Chinese technology ecosystem; if it stays engaged, it denies that ecosystem a foothold on the EU's own border.[67]

For Turkey, convergence would turn regulatory alignment from a constraint into an asset. Compatible rules lower compliance costs and secure access to a larger market, while association instruments such as the Digital Europe Programme and Horizon Europe transfer capabilities that indigenization alone cannot generate.[68] Interoperable standards hedge against vendor lock-in when considering digital networks and clouds. Legal certainty is itself industrial policy, since legal uncertainty is reportedly among the leading reasons Turkish firms hold back from adopting artificial intelligence. An AI framework compatible with the European one would therefore unlock domestic adoption rather than merely please Brussels. Finally, a credible European anchor strengthens rather than dilutes the country's ambition to be recognized as a technology exporter.

Jointly, enhanced cooperation between the two sides would help both actors gain what neither can produce alone. One gain is cyber resilience across infrastructure that is already interconnected, from energy to finance to transport—where incidents cascade regardless of doctrine. The larger gain would be the foundation of a regional digital ecosystem that pools market scale, infrastructure, standards, and talent, giving the two actors the collective weight to bargain with digital superpowers such as the United States and China rather than merely choose between them. It also gives the EU and Turkey a stronger voice in global standard-setting as a third pole of rules and capabilities. The instruments are within reach, since cooperation can proceed along a market track covering supply-chain security, interoperability, and certification; an innovation track using Digital Europe clusters, testbeds, regulatory sandboxes, and skills academies; and a technical and regulatory track built on structured dialogue, common vulnerability-scoring frameworks, trusted channels between national incident-response teams, and joint exercises. A standing EU–Turkey cyber dialogue would sit above these three tracks and coordinate them. It would also house the machinery that is the real missing layer: institutional trust-building through joint supervisory bodies, data-flow agreements, and mutual recognition mechanisms anchored to the Customs Union. As confidence matures, the cybersecurity objective of the Digital Europe Programme could be opened to Turkey.

One qualification remains. Without common values and shared policy objectives, convergence stays fragile. Deep cooperation in the most sensitive layers of the digital stack, cybersecurity, data flows, and critical infrastructure will therefore require treating fundamental-rights safeguards, transparency, and oversight not as external conditionality imposed on Turkey but as the trust infrastructure that makes sensitive cooperation possible for both sides.

Conclusion

Turkey's 5G launch on April 1, 2026, and the Commission's Tech Sovereignty package of June 3, 2026, aspire to reach the same objects under the same constraints. Digital sovereignty, this analysis has argued, is best understood relation-

ally, as a claim to control data, infrastructure, supply chains, platforms, technologies, standards, and skills that can only ever be exercised through interdependence, never against it. The EU has built a normative answer to that constraint, Turkey a local technological-oriented one. Their divergence is acute, spanning the philosophy of control, referent objects, governance culture, asymmetry, and trust. Yet there are compatibilities: from a shared structural position to convergent threat framings, overlapping legal orders, and economies integrated through the Customs Union since 1996. This is why the current condition can be described as convergence on paper without a relationship to match.

It is precisely that relational gap that a convergent approach would close. For the EU, Turkey is the test of whether regulatory sovereignty can be an offer rather than an imposition; for Turkey, the EU is the test of whether technological self-reliance can mature from import substitution into interoperable capacity. Both already know what their own strategists avoid saying aloud: that under conditions of technological bipolarity the choice is not between sovereignty and dependence but between negotiated and unnegotiated interdependence. Managed interdependence built on shared standards, pooled skills, resilient supply chains, and rights-based trust infrastructure is not the abandonment of digital sovereignty. It is the only version of it that either actor can actually obtain: Sovereign but not alone.

Acknowledgements

This paper grew out of the panel “Digital Sovereignty and Strategic Autonomy in Cyberspace: Perspectives from the European Union and Turkey,” which I convened and moderated at Istanbul Policy Center (IPC), Sabancı University, on May 11, 2026, as a 2025/26 Mercator–IPC Fellow. I am especially grateful to the panelists, Linda Monsees (Institute of International Relations, Prague), Ayhan Gücüyener Evren (Nişantaşı University, Istanbul), and Zeynep Ayata (Istanbul Policy Center), whose presentations on “The EU’s Digital Sovereignty Strategy,” “Turkey’s Digital Strategic Autonomy Ambitions,” and “Coordination and Conflict in Approaching Cyberspace,” respectively, informed several of the arguments developed here. My thanks also go to all the participants in the discussion that followed. The views expressed here and any errors are mine alone.

Notes

1 | "5G'de Geri Sayım Başladı," T.C. Ulaştırma ve Altyapı Bakanlığı, August 31, 2025, https://www.uab.gov.tr/haberler/5g-de-geri-sayim-basladi; "Türkiye mobil iletişimde 5G teknolojisine geçti," *TechnoLogic*, March 31, 2026, https://www.technologic.com.tr/turkiye-mobil-iletisimde-5g-teknolojisine-gecti/82580/.html. The Ministry of Transport and Infrastructure announced domestic-content ("yerlilik ve millilik") ratios of up to 60% for the 5G build-out.

2 | European Commission, "Strengthening Europe's Tech Sovereignty," *Shaping Europe's Digital Future*, accessed July 17, 2026, https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty; European Commission, "Strengthening Europe's Tech Sovereignty," June 3, 2026, https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en.

3 | European Commission, "Strengthening Europe's Tech Sovereignty."

4 | Linda Monsees, remarks at the panel discussion "Digital Sovereignty & Strategic Autonomy in Cyberspace: Perspectives from the European Union and Turkey" (Istanbul Policy Center, Sabancı University, Istanbul, May 11, 2026).

5 | Julia Pohle and Thorsten Thiel, "Digital Sovereignty," *Internet Policy Review* 9, no. 4 (2020), https://doi.org/10.14763/2020.4.1532; Rocco Bellanova, Helena Carrapico, and Denis Duez, "Digital/Sovereignty and European Security Integration: An Introduction," *European Security* 31, no. 3 (2022): 337–355, https://doi.org/10.1080/09662839.2022.2101887.

6 | Catherine Morin-Desailly, *L'Union européenne, colonie du monde numérique?* Rapport d'information no. 443 (2012–2013) (Paris: Sénat, March 20, 2013), https://www.senat.fr/rap/r12-443/r12-443.html; The German Presidency of the EU Council, *Together for Europe's Recovery: Programme for Germany's Presidency of the Council of the European Union* (Berlin, 2020), 8, discussed in Pohle and Thiel, "Digital Sovereignty."

7 | European Commission, "Strengthening Europe's Tech Sovereignty."

8 | Stéphane Couture and Sophie Toupin, "What Does the Notion of 'Sovereignty' Mean When Referring to the Digital?" *New Media & Society* 21, no. 10 (2019): 2305–2322; Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology* 33 (2020): 369–378.

9 | Mauro Santaniello, "Attributes of Digital Sovereignty: A Conceptual Framework," *Geopolitics* 31, no. 2 (2026): 788–809, https://doi.org/10.1080/14650045.2025.2521548.

10 | Pohle and Thiel, "Digital Sovereignty."

11 | Santaniello, "Attributes of Digital Sovereignty," 789; Tambiama Madiega, *Digital Sovereignty for Europe*, EPRS Briefing PE 651.992 (Brussels: European Parliamentary Research Service, 2020).

12 | Monsees, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

13 | Ibid.

14 | Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999); on hypocrisy as a structural attribute of digital sovereignty claims, Santaniello, "Attributes of Digital Sovereignty," 801–802.

15 | Monsees, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

16 | Andrew B. Kennedy and Darren J. Lim, "The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century," *International Affairs* 94, no. 3 (2018): 553–572.

17 | Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42–79.

18 | Santaniello, "Attributes of Digital Sovereignty," 794–800.

19 | Monsees, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

20 | Ayhan Gücüyener Evren, remarks at the panel discussion "Digital Sovereignty & Strategic Autonomy in Cyberspace: Perspectives from the European Union and Turkey" (Istanbul Policy Center, Sabancı University, Istanbul, May 11, 2026).

21 | Mario Draghi, *The Future of European Competitiveness* (Brussels: European Commission, September 2024).

22 | Council of the European Union, "Declaration for European Digital Sovereignty," ST 15781/25 (Brussels, November 27, 2025), https://data.consilium.europa.eu/doc/document/ST-15781-2025-INIT/en/pdf; Council of the European Union, "Summit on European Digital Sovereignty (Berlin, November 18, 2025)," ST 16186/25 (Brussels, December 2, 2025), https://data.consilium.europa.eu/doc/document/ST-16186-2025-INIT/en/pdf; European Commission, *Cloud Sovereignty Framework*, version 1.2.1 (Brussels, October 20, 2025); "Sovereign Cloud Framework Explained," European Commission, June 1, 2026, https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en.

23 | Jakub Eberle and Linda Monsees, "Digital Sovereignty and Central and Eastern Europe: Agency, Structural Disadvantage and Digital Politics at EU's (Semi-)Periphery," *Journal of Contemporary European Studies* 34, no. 2 (2026), https://doi.org/10.1080/14782804.2025.2610601.

24 | Ursula von der Leyen, *A Union That Strives for More — My Agenda for Europe: Political Guidelines for the Next European Commission 2019–2024* (Brussels, 2019).

25 | "'Strategic Autonomy for Europe — The Aim of Our Generation': Speech by President Charles Michel to the Bruegel Think Tank," Council of the EU, September 28, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/09/28/l-autonomie-strategique-europeenne-est-l-objectif-de-notre-generation-discours-du-president-charles-michel-au-groupe-de-reflexion-bruegel/.

26 | Notably Regulation (EU) 2016/679 (General Data Protection Regulation); Regulation (EU) 2022/1925 (Digital Markets Act); Regulation (EU) 2022/2065 (Digital Services Act); Regulation (EU) 2024/1689 (Artificial Intelligence Act); Directive (EU) 2022/2555 (NIS2); Regulation (EU) 2024/2847 (Cyber Resilience Act); and Regulation (EU) 2022/2554 (DORA).

27 | "EU AI Act Unpacked #34: The Final Digital Omnibus on AI — Key Amendments to the AI Act and Their Impact on Businesses Active in the EU," Freshfields, July 2026, https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/eu-ai-act-unpacked-34-the-final-digital-omnibus-on-ai-key-amendments-to-the-a-102nber. The amendments, endorsed by the European Parliament on June 16 and by the Council on June 29, 2026, defer the high-risk regime to December 2, 2027, for

stand-alone systems and to August 2, 2028, for embedded systems, while most transparency obligations under Article 50 still apply from August 2, 2026.

28 | European Commission, "EU Cybersecurity Policies," *Shaping Europe's Digital Future*, accessed July 17, 2026, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies (on the cybersecurity package proposed on January 20, 2026); European Commission, "Strengthening Europe's Tech Sovereignty."

29 | Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020).

30 | Dennis Broeders, Fabio Cristiano, and Monica Kaminska, "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions," *JCMS: Journal of Common Market Studies* 61, no. 5 (2023): 1261–1280.

31 | Benjamin Farrand and Helena Carrapico, "Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity," *European Security* 31, no. 3 (2022): 435–453.

32 | Zeynep Ayata, remarks at the panel discussion "Digital Sovereignty & Strategic Autonomy in Cyberspace: Perspectives from the European Union and Turkey" (Istanbul Policy Center, Sabancı University, Istanbul, May 11, 2026).

33 | Monsees, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

34 | Draghi, *The Future of European Competitiveness*.

35 | Freshfields, "EU AI Act Unpacked #34."

36 | "Millî Teknoloji Hamlesi," Türkiye Teknoloji Takımı Vakfı, accessed July 17, 2026, https://www.t3vakfi.org/tr/hakkimizda/mth/; "Sıkça Sorulan Sorular," TEKNOFEST, accessed July 17, 2026, https://teknofest.org/tr/kurumsal/sss/.

37 | "Milli Teknoloji Hamlesi'nde yeni eşik: Hedef 100 milyar dolar," Bigpara/Anadolu Ajansı, May 22, 2026, https://bigpara.hurriyet.com.tr/haberler/teknoloji-haberleri/milli-teknoloji-hamlesinde-yeni-esik-hedef-100-milyar-dolar_ID100871959/.

38 | Gücüyener Evren, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

39 | Ibid.

40 | North Atlantic Treaty Organization, "Warsaw Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8–9 July 2016," July 9, 2016.

41 | Ulaştırma ve Altyapı Bakanlığı, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024–2028* (Ankara: Ministry of Transport and Infrastructure, 2024).

42 | Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi, *Resmî Gazete* no. 32776, January 8, 2025, https://www.resmigazete.gov.tr/eskiler/2025/01/20250108-1.pdf.

43 | Siber Güvenlik Kanunu, Law No. 7545, *Resmî Gazete* no. 32846, March 19, 2025, https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm. Among the law's stated principles, to ensure cybersecurity, "domestic and national products shall be preferred as a priority [*öncelikle yerli ve milli ürünler tercih edilir*]." On Law No. 7545 as Türkiye's first comprehensive cybersecurity legislation, "Turkey: Data Protection & Cyber-

security," *The Legal 500 Country Comparative Guides*, accessed July 27, 2026, https://www.legal500.com/guides/chapter/turkiye-data-protection-cybersecurity/.

44 | Cumhurbaşkanlığı Kararnamesi No. 192, December 25, 2025; "Siber Güvenlik Başkanlığının Yetki Alanını Genişleten Kanun Teklifi TBMM'ye Sunuldu," Pekin Bayar Mizrahi, July 7, 2026, https://pekin.com.tr/2026/07/07/siber-guvenlik-baskanliginin-yetki-alanini-genisleten-kanun-teklifi-tbmmye-sunuldu/ (on the bill of July 3, 2026, and on the transitional rules pending the law's secondary regulations); Forseti Hukuk Bürosu, "Siber Güvenlik Kanunu: 9 Ay Sonra Neredeyiz?" (noting that no implementing regulation had been issued as of late 2025).

45 | Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Law No. 7499, *Resmî Gazete* no. 32487, March 12, 2024; Hilal Temel, "Navigating Türkiye's Updated International Data Transfer Rules: What You Need to Know," Slaughter and May – The Lens, January 31, 2025, https://thelens.slaughterandmay.com/post/102jxqd/navigating-turkiyes-updated-international-data-transfer-rules-what-you-need-to.

46 | Republic of Türkiye, Directorate for EU Affairs, "Dijital Avrupa Programı," accessed July 17, 2026, https://www.ab.gov.tr/dijital-avrupa-programi-digital-europe-_53088.html (noting that Türkiye does not take part in the program's cybersecurity component owing to security restrictions); "Digital Europe Program Participation Agreement Signed," IPA, September 2023, https://ipa.gov.tr/en/digital-europe-program-participation-agreement-signed/ (agreement signed on August 31, 2023).

47 | For a comparison of the three artificial intelligence bills before the Grand National Assembly as of 2026, "Türkiye'de 2026 Yapay Zekâ Kanunu: TBMM'ye Sunulan Üç Kanun Teklifinin Detaylı Karşılaştırılması," NPartners, 2026, https://npartners.com.tr/tr/turkiyede-2026-yapay-zeka-kanunu-tbmmye-sunulan-uc-kanun-teklifinin-detayli-karsilastirilmasi.

48 | "TBMM Yapay Zeka Araştırma Komisyonu Başkanı Dönmez, komisyonun raporuna ilişkin basın toplantısı düzenledi," TBMM Haber, March 26, 2026, https://www.tbmm.gov.tr/Haber/Detay?Id=a5cf661f-e7c5-47e6-a9ae-019d2b862b3c; "Komisyondan 'Türkiye Yapay Zeka Kurumu' önerisi," *DHA*, March 26, 2026, https://www.dha.com.tr/yerel-haberler/ankara/komisyondan-turkiye-yapay-zeka-kurumu-onerisi-2843557.

49 | "e-Devlet'te 68 milyon kullanıcı," *Hürriyet*, February 2, 2026, https://www.hurriyet.com.tr/gundem/e-devlette-68-milyon-kullanici-43097928; Ayata, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

50 | Fırat Akan and Bared Çil, *Türkiye's E-Government Track Record: Digital Transformations Inspiring Europe*, İKV Brief (Istanbul: İktisadi Kalkınma Vakfı, n.d.), accessed July 17, 2026, https://www.ikv.org.tr/images/files/ikv_brief_turkiye_egovernment_digital_transformation_firat_akan_bared_cil.pdf.

51 | "TBMM Yapay Zeka Araştırma Komisyonu Başkanı Dönmez," TBMM Haber; "Komisyondan 'Türkiye Yapay Zeka Kurumu' önerisi," *DHA*.

52 | Senem Aydın-Düzgit, Mustafa Kutlay, and E. Fuat Keyman, "Strategic Autonomy in Turkish Foreign Policy in an Age of Multipolarity: Lineages and Contradictions of an Idea," *Inter-*

national Politics 63 (2026): 184–205, https://doi.org/10.1057/s41311-024-00638-w.

53 | Ayata, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

54 | European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 final (Brussels, December 16, 2020).

55 | Siber Güvenlik Kanunu, Law No. 7545.

56 | Ayata, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

57 | Republic of Türkiye, Directorate for EU Affairs, "Dijital Avrupa Programı."

58 | European Commission, *Türkiye 2025 Report*, SWD(2025) 756 final (Brussels, November 4, 2025), https://enlargement.ec.europa.eu/turkiye-report-2025_en.

59 | Pohle and Thiel, "Digital Sovereignty."

60 | Santaniello, "Attributes of Digital Sovereignty," 794–800.

61 | Compare European Commission and High Representative, *The EU's Cybersecurity Strategy for the Digital Decade*, with Siber Güvenlik Kanunu, Law No. 7545.

62 | Compare Siber Güvenlik Kanunu, Law No. 7545, and Law No. 7499 with, respectively, Directive (EU) 2022/2555 and Regulation (EU) 2016/679; on the draft AI law, Yapay Zeka Kanunu Teklifi, TBMM Esas No. 2/2234, submitted June 24, 2024, arts. 3–6, https://www.tbmm.gov.tr/Yasama/KanunTeklifi/e21539a0-888a-4500-81be-01904a918c53; and Selen Dogan Kosterit, "AI Policy Corner: The Turkish Artificial Intelligence Law Proposal," Montreal AI Ethics Institute, March 17, 2025, https://montrealethics.ai/ai-policy-corner-the-turkish-artificial-intelligence-law-proposal/; Ayata, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

63 | Eurostat, "EU High-Tech Trade: Exports Up in 2023," October 4, 2024, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20241004-1; Delegation of the European Union to Türkiye, "EU and Türkiye Deepen Cooperation in Industrial Decarbonisation and Innovation Policy," November 27, 2025, https://www.eeas.europa.eu/delegations/turkiye/eu-and-turkiye-deepen-cooperation-industrial-decarbonisation-and-innovation-policy_en?s=230.

64 | Monsees, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

65 | Ayata, remarks, "Digital Sovereignty & Strategic Autonomy in Cyberspace."

66 | Bradford, *The Brussels Effect*.

67 | On the vendor landscape, Güntay Şimşek, "5G'nin ne kadarı milli, yerli, ithal olacak?" *Haber Aero*, February 20, 2026, https://mail.haber.aero/yazarlar/guntay-simsek/5gnin-ne-kadari-milli-yerli-ithal-olacak/.

68 | Republic of Türkiye, Directorate for EU Affairs, "Dijital Avrupa Programı."

About the Istanbul Policy Center-Sabancı University-Stiftung Mercator Initiative

The Istanbul Policy Center–Sabancı University–Stiftung Mercator Initiative aims to strengthen the academic, political, and social ties between Turkey and Germany as well as Turkey and Europe. The Initiative is based on the premise that the acquisition of knowledge and the exchange of people and ideas are preconditions for meeting the challenges of an increasingly globalized world in the 21st century. The Initiative focuses on two areas of cooperation, EU/German-Turkish relations and climate change, which are of essential importance for the future of Turkey and Germany within a larger European and global context.

Jacopo Franceschini is a 2025/26 Mercator–IPC Fellow.

The interpretations and conclusions made in this paper belong solely to the author and do not reflect IPC's official position.

Digital Geopolitics and Sovereignty: Convergence and Divergence between the EU and Turkey
17 p.; 25 cm. - (Istanbul Policy Center-Sabancı University-Stiftung Mercator Initiative)

Cover Design and Page Layout: MYRA

Istanbul Policy Center
Bankalar Caddesi Minerva Han No: 2 Kat: 4
34420 Karaköy-İstanbul
T +90 212 292 49 39
ipc@sabanciuniv.edu - ipc.sabanciuniv.edu

IPC | ISTANBUL POLICY CENTER
SABANCI UNIVERSITY
STIFTUNG MERCATOR INITIATIVE