

The Paradox of European Digital Sovereignty: Between Liberal Defence and Regulatory Fragmentation

Samir ELBAH

University of Batna1, (Algeria)

Samir.elbah@univ-batna.dz

Abstract ;

This study examines European digital sovereignty as a central element of contemporary geopolitical competition. It focuses on the tension between the European Union's commitment to maintaining a liberal, open, and interoperable digital space and the geopolitical imperative to defend against the "weaponisation of dependencies." The study investigates whether the EU's pursuit of digital sovereignty generates a structural tension between liberal openness and digital fragmentation (Splinternet). It argues that defensive strategies aimed at reducing technological dependencies may deepen fragmentation by creating regulatory and legal barriers. The study employs a qualitative analytical methodology combining policy analysis, a case study of 5G technology, and a comparative analysis of European, American, and Chinese models. The results show that the EU's regulatory instruments, particularly the GDPR, DSA, and DMA, have strengthened its regulatory power while simultaneously contributing to digital fragmentation. These findings highlight a fundamental dilemma between strengthening strategic autonomy and preserving an open and interoperable digital space.

Article info

Received

April 30.2026

Accepted

September 09.2026

Keyword:

- ✓ Digital sovereignty
- ✓ The European model
- ✓ The weaponisation of dependencies
- ✓ Digital fragmentation

1. Introduction

The digital sphere and the technological sphere in general is undergoing a profound qualitative transformation, shifting from a borderless domain based on openness and the free flow of information to a space in which the stakes of sovereignty and control are rising. This transformation is no longer merely a technical development; rather, it reflects a reshaping of the international system's architecture against a backdrop of escalating geopolitical competition and growing reliance on digital infrastructure as a fundamental pillar of power and influence.

A series of accelerating international shifts such as the COVID-19 pandemic, the war in Ukraine, and rising tensions between major powers, particularly between the European Union and the United States on the one hand, and China on the other — have contributed to highlighting the centrality of the digital issue and transforming it into one of the main pillars of the international agenda. In this context, the concept of 'the weaponisation of interdependence' has emerged as an interpretative framework for understanding how networks of economic and technological interdependence have become tools for geopolitical pressure and influence, thereby redefining the relationship between globalisation and sovereignty.

Within this shift, digital sovereignty is no longer reduced to its technical or economic dimensions, but has become a political and legal issue with normative dimensions, relating to the projection of governance models and values within the digital space. In this context, the European Union stands

out as an actor seeking to reposition itself within the global digital system by adopting an ambitious strategy to strengthen 'digital sovereignty', based on reducing critical dependencies and strengthening autonomy in technological decision-making, whilst maintaining a digital model grounded in liberal values such as data protection, openness and interoperability.

However, this strategy raises a central problem concerning its contradictory nature. On the one hand, the European Union presents itself as a defender of an open and global digital model; on the other, it relies on centralised regulatory and security tools based on control over data and digital infrastructure. Herein lies a fundamental structural paradox: the logic of protection converges with the logic of control, raising serious questions about the extent to which this model can maintain its internal balance in a competitive international environment.

Building on this, the study examines the contribution of the European Union's digital sovereignty strategy, against the backdrop of the 'weaponisation of dependencies', to the entrenchment of a contradiction between the logic of digital openness and the requirements of control and regulation, and the consequent deepening of the 'Splinternet' phenomenon. This study posits that the European Union's adoption of digital sovereignty policies, in the context of the escalating 'weaponisation of dependencies', is not merely a defensive response, but structurally contributes to the production of new forms of 'regulatory fragmentation' by imposing extra-

territorial legal standards that redraw the boundaries of the global digital space.

To test this hypothesis, the study adopts an analytical approach that combines legal and geopolitical dimensions, by analysing the European regulatory framework—particularly legislation issued by the European Commission—and interpreting its implications in light of shifts in the international system, using the case study of 5G (5G) as an applied model highlighting the overlap between technological sovereignty and interdependence.

Accordingly, the study is divided into four main sections: the first addresses digital sovereignty as a geopolitical phenomenon linked to the militarisation of dependencies; the second analyses the competition between political and value-based models in the governance of the digital space; the third focuses on the dilemma of balancing sovereignty and interdependence through the case of 5G; and the fourth is devoted to examining the phenomenon of the ‘Splinternet’ in the light of the European strategy, with a view to identifying the limitations of this model and its future prospects.

2. Digital sovereignty as a geopolitical phenomenon – the weaponisation of digital dependencies and platforms:

Digital sovereignty has become an important source of friction in contemporary geopolitical relations. This development was reinforced during the COVID-19 pandemic and through its broader repercussions. Two dimensions are particularly relevant. The first concerns the growing influence of geo-economic factors

in international relations and the exploitation of critical economic and technological dependencies. Globalisation has created extensive networks involving financial and technological flows, agricultural commodities, energy, and information infrastructures, which can increasingly be used as instruments of geopolitical pressure. From this perspective, coercive economic measures, such as sanctions, can function as instruments of geopolitical competition alongside other forms of statecraft (Farrell & Newman, 2019, pp. 44-48).

Digital sovereignty can broadly be understood as the capacity of a state or political entity to exercise effective control, regulatory authority, and strategic autonomy over critical digital infrastructures, technologies, data, and related dependencies. Unlike traditional sovereignty, it raises distinctive challenges associated with reliance on foreign technology providers, control over personal data, and the security and resilience of information systems (Lee, 2025).

Digital sovereignty has become one of the inevitable points of friction in geopolitical relations. This characteristic has been clearly reinforced during the pandemic crisis and through its manifold repercussions. There are two aspects to these repercussions: the first concerns the growing influence of the geo-economic factor in international relations, which extends beyond the digital economy to encompass the ‘weaponisation’ of key economic dependencies. In other words, the factors of globalisation – financial and technological flows, exports of agricultural

raw materials and energy, as well as information networks – are being used as weapons. According to this approach, coercive economic measures – such as sanctions – are no longer an alternative to war, but rather an extension of it. The concept of "weaponised interdependence," as developed by Henry Farrell and Abraham Newman (2019, pp. 42-79), provides a crucial analytical framework for understanding these dynamics. The argument is that states can exploit their positions within global networks of economic and technological interdependence to coerce others. The United States, for example, has used its control over key nodes in semiconductor supply chains, cloud computing infrastructure, and financial messaging systems to exert pressure on adversaries. Farrell and Newman's subsequent book, **Underground Empire** (2024), explores how the United States has built and utilized global economic, financial, and technological networks for geopolitical purposes, highlighting the control of infrastructures such as finance, submarine cables, data centers, and semiconductors as the basis of this "underground empire".

The aim is to deplete the resources the enemy can mobilise for combat, thereby increasing the economic burden of war, as well as to weaken the morale of the opposing population to undermine their capacity for resistance and support for the government. (Farrell, 2019, pp. 44–48)

Digital sovereignty refers to the ability of a state, organization or individual to control its infrastructure, technologies and data within cyberspace. Unlike traditional sovereignty, digital sovereignty poses new challenges related to reliance on foreign

technology providers, control over personal data, and ensuring the security of information systems. (Lee, 2025)

In this context, digital sovereignty can constitute a political and industrial response to external pressure, whether from the perspective of 'self-sufficiency' (a term used by the Chinese authorities since 2015) or 'import substitution' (a term used by Moscow since 2014). In the case of Russia specifically, digital or technological sovereignty has since been invoked to circumvent international sanctions, particularly in the strategic semiconductor industry, where Russia lacks its own production capabilities (especially for the most complex components) and a sovereign value chain. The country relies primarily on ARM architectures for the processors designed by Baikal Electronics and on production tools provided by the Taiwanese company TSMC. (Nocetti, 2023)

With regard to manufacturing precision (*finesse de gravure*), which remains the most widely used benchmark for assessing the level of development of the semiconductor industry, the Russian sector offers products with transistor precision ranging from 16 to 28 nanometres (nm), as for actual production, the manufacturing lines are unable to go below 90 nanometres. The fact is that the 90-nanometre level was the norm in Western countries during 2004–2005, and is the same level used, for example, in the PlayStation 3, which highlights the extent of the lag suffered by this sector in Russia. By contrast, the world's most advanced production lines today reach 10, 7 and even 5 nanometres, and there is already talk of the next generation at 3 and even 2

nanometres. ARM is often described as a key hub in the semiconductor industry. In other words, even if Russia were to infringe upon ARM's industrial property rights in order to produce microchips, it would be unable to manufacture them with a precision of between 16 and 28 nanometres, as it lacks the necessary industrial infrastructure. (Thys, 2022)

These foreign companies have complied with international sanctions policies, exposing Russia to the risk of component shortages—a risk that its Chinese partner may not be prepared to bear, given that it too faces US sanctions on processor supplies. The US and its allies have accused China of supporting Russia's war in Ukraine, partly by exporting parts and equipment needed by Moscow's arms factories. The US State Department and Treasury Department have imposed several rounds of sanctions on entities around the world with alleged commercial links to the Russian military, including front companies in Hong Kong that were diverting semiconductors. The decline in illicit flows resulted from several factors, including robust enforcement by US authorities, as well as engagement with companies whose products are being re-exported. (Pomfret, 2024)

The second aspect concerns the interactions between mainstream digital platforms and states. These platforms played a pivotal role during the COVID-19 crisis in ensuring the continuity of connections between states, individuals and organisations. They are not limited to shaping political and social relations; today, they are at the heart of power struggles. Competition, cooperation and

conflict between China and the United States, in particular, play out through these platforms. (Nardon, 2021)

The issue of regulating the “the GAFAM companies—Google, Apple, Meta (formerly Facebook), Amazon, and Microsoft—digital giants is increasingly seen – particularly in Europe – as a means of establishing the digital sovereignty that the continent has long lacked. Consequently, it is becoming a classic issue in international relations, one that may regularly spark controversy and strain relations between allies (such as the European Union and the United States). Since 2019, the European Union has made the taxation of GAFAM companies one of the key political pillars of the ‘Geopolitical Commission 2020’. The various European initiatives in this area have been framed as part of efforts to defend Europe's ‘digital sovereignty’ in the face of the exploitative technological and innovation strategies of the American and Chinese systems. (Commission., 2020)

3. Digital sovereignty as a model issue – competition between political and value models:

Digital sovereignty is not merely an internal matter, but also concerns the projection of a vision and model at the international level. In this context, part of the current debate centres on the clash of values between the approach championed by liberal democracies and that put forward by authoritarian states. (CIGREF, 2024, p. 74)

More specifically, the dividing line is divided into two levels. The first concerns the degree to which digital ecosystems are open to global dependencies – or, at the

very least, the ability of those states to control their critical dependencies. Since the late 1990s, authoritarian regimes such as China, Russia and Iran have, to varying degrees, sought to free themselves from their dependence on American technologies, which they view as a means of interference and potentially sabotage. The adoption of a trend towards politically defined technological ecosystems will undermine the open spirit that nourishes and benefits freer societies – and reinforce the top-down, controlling spirit favoured by repressive regimes. And if competitors are less interconnected and interdependent, they will have less incentive to refrain from launching attacks on each other's critical infrastructure. (Fiott, 2020, pp. 2–3)

The second-dimension concerns divergent interpretations of the very concept of 'digital sovereignty'. The internet, which defies subjugation to any form of authority, is not universally viewed globally as a medium that must necessarily promote the liberation of peoples. Here, the focus is on what is known as the 'knowledge layer' of the internet, which is the subject of this approach. Contrary to the European conception, digital sovereignty as understood in both Russia and China focuses on safeguarding the 'national' information space from foreign influences deemed subversive, whilst keeping pace with international trends that have emerged over the past decade, such as data repatriation and the strengthening of digital infrastructure. This Sino-Russian approach is also characterised by an unhesitating recourse to the law, which is employed in various ways to reinforce the primacy of political decision-making in the digital sphere and to ensure the stability, and

indeed the very survival, of the regimes. In both countries, the 'securitization' of the national digital space has been manifested through the adoption of a discourse based on existential threats, to justify the adoption of measures and procedures that are more restrictive of freedom of expression and assembly. Once again, opposition to US policy—which is based on promoting the free flow of information and granting a central role to the private sector—constitutes one of the key determinants of these states' political stance. (Nocetti, 2023, p. 20.)

The model of digital authoritarianism is becoming increasingly prominent in international debates, as it reflects a contrasting conception of sovereignty in the digital sphere. In this context, Russia has been working since the late 1990s to promote the concept of 'information sovereignty' within the United Nations, particularly since 1998, seeking to win over states that are wary of the free flow of information model supported by the United States, and to push them towards adopting a more sovereign approach to digital governance (J., 2015, pp. 111–130).

As a dividing line in debates on global internet governance, the concept of 'sovereignty' is also exploited by these states for foreign policy purposes. For example, prior to its ban in the European Union from March 2022, the Russian state-run channel RT broadcast programmes and articles in France pointing to the "absence" of digital sovereignty in Europe, whilst highlighting various spying scandals involving allies, thereby fuelling already polarised debates concerning the United States. Beyond this divergence linked to the nature of the systems, the European

approach, according to a complex spectrum, is characterised by its own political line. The absence of prominent European digital players is driving the European Union to defend a specific model of a digital society centred on values such as personal data protection, fair competition and adequate taxation, the defensive dimension of which is sometimes viewed as a form of anti-Americanism. (Nocetti J., 2024, pp. 74–75.)

In February 2021, Charles Michel, President of the European Council, stated that “there is no strategic autonomy without digital sovereignty”, thereby formally placing at the heart of the debate the concept of “strategic autonomy”, which carries security and perhaps military connotations – here applied to digital policy and data infrastructure. (CIGREF, 2024, p. 118)

The emphasis on the ambition of “autonomy” points to a geopolitical interpretation aimed at enabling the European Union to compete with the two digital superpowers, China and the United States, whilst protecting its vital interests. However, not all Member States support the development of

European strategic autonomy; those that do not agree on its content or on the level of geographical and functional ambition that should be adopted to implement it. The stance towards the United States lies at the heart of discussions on European strategic autonomy and constitutes a point of friction regarding the risks it may pose to transatlantic relations, particularly in the field of defence. The emphasis on autonomy therefore has a geopolitical dimension, enabling the European Union to

protect its vital interests while seeking to compete with major technological powers such as China and the United States. Nevertheless, Member States do not necessarily share identical views regarding the content or scope of European strategic autonomy. The relationship with the United States remains particularly important, given concerns about the implications of greater European autonomy for transatlantic relations, especially in the field of defence. (Nocetti J., 2023, pp. 20–21)

Digital sovereignty policies increasingly involve the projection of values and political models internationally. The European Union, in particular, has sought to use its regulatory power to promote its values globally, including privacy protection, competition, and democratic accountability. This "normative power" dimension of European digital sovereignty is significant not only for its impact on EU member states but also for its influence on global digital governance (Bradford, 2020).

The concept of the "Brussels Effect," as developed by Anu Bradford (2020), provides an analytical framework for understanding how EU regulatory standards can extend beyond the Union's territory. The combination of market size, regulatory capacity, and the incentives of multinational firms to adopt common standards enables the EU to exert significant influence on global regulatory developments. The GDPR, for example, has influenced privacy legislation in numerous countries, including Brazil, Japan, India, and South Korea, creating a

"de facto" global standard for data protection (Bradford, 2020).

However, the projection of European values also creates tensions. The extraterritorial reach of EU regulations may be perceived as a form of regulatory imperialism by other states, particularly those with different value systems. The EU's insistence on privacy protection, for example, has created conflicts with the United States over data transfers and with China over data localization requirements. The tension between promoting European values and respecting other states' sovereignty and cultural differences is a persistent challenge (Colbert, 2026).

4. The balance between sovereignty and interdependence – the case of 5G

Discussions on digital sovereignty have often centred on answering the question 'Who controls the internet?'. These debates have since broadened thanks to the massive expansion of the digital sphere driven by the development and proliferation of emerging (or sensitive) technologies, such as artificial intelligence, 5G networks and quantum technologies. It has therefore become essential to broaden the scope of consideration, adding the issue of control over sensitive algorithms, as well as the issue of the supply of sensitive components, which has become one of the most prominent current developments. (Nocetti J., 2023, p. 5)

In fact, the expansion of the sphere of digital sovereignty has led to an unmistakable overlap between the industrial and geopolitical dimensions.

This is particularly evident in the field of semiconductors, where China continues its efforts to achieve self-reliance and technological catch-up in advanced semiconductors. However, this sector remains the weakest link in China's innovation-driven development strategy. Beijing's ambitions in this field have never translated into any form of leadership, whether since the '531 Plan' of 1986 or through the \$50 billion fund allocated to integrated circuits in 2014. Chinese manufacturers lack a sufficiently robust industrial base and technical expertise in this sector, particularly in the most advanced components, making electronic chips the country's top import item, surpassing even fossil fuels. (A., 2021)

Geopolitical factors limit China's ability to catch up in the short term, despite its reliance on its progress in artificial intelligence (AI) to bridge this gap. Nevertheless, the announced figures, which estimate Chinese government support for the sector at over \$290 billion between 2021 and 2022, evoke a sense of both dizziness and a comprehensive confrontation over control of production and supply chains. (J. L., 2023)

In Europe, the power struggle between nations (Germany, France, and others) to attract Taiwanese and American investment with the aim of (very partially) relocating the production fabric to the continent requires an analysis of contemporary technological policies that take the geopolitical dimension into account, as well as a critique of the pitfalls arising from over-reliance on a 'fables' manufacturing model, with its inherent structural dependence within production chains. (Nocetti J., 2023, p. 5)

Discussions surrounding 5G have raised questions about the balance and future of the relationship between global interdependence and the stated ambitions of sovereignty or strategic independence in the technological sphere. In this regard, digital sovereignty and technological sovereignty are often conflated when it comes to 5G. Whilst digital sovereignty is associated with a long list of concerns (loss of control over data, cybersecurity risks, digital competition in the provision of public services, threats to civil liberties and democratic values), technological sovereignty encompasses the former but refers more broadly to Europe's loss of autonomy in key technologies for strategic sectors, such as the defence industry and telecommunications infrastructure, or for the future, such as artificial intelligence and the Internet of Things. (Nocetti J., 2023, p. 21)

Traditionally, two interpretations clash when considering European 'sovereignty' in the technological sphere. One view considers Europe to be 'subordinate', as it lacks the capacity for political and economic independence in this regard. The second interpretation, however, believes in Europe's ability to operate in the digital sphere and in vital technologies, thanks to the development of high-level scientific expertise and the uniqueness of a governance model based on European values. (J. N., 2021, pp. 51–63)

In reality, it is impossible to distinguish between these two interpretations; the European Union knows how to capitalize on its technological superiority, yet it faces the unforeseen geopolitical challenges of its political project, which are sometimes

starkly reflected in the international technological arena. With 5G, the most notable change concerns the Chinese issue.

The 5G debate makes this relationship between sovereignty and interdependence particularly visible. Digital sovereignty and technological sovereignty are often conflated in discussions of 5G, although they refer to overlapping but distinct dimensions. Digital sovereignty primarily concerns control over data, digital infrastructures, cybersecurity, and regulatory conditions, whereas technological sovereignty extends to the capacity to develop, produce, and secure critical technologies and supply chains. The 5G case illustrates how these dimensions increasingly overlap, particularly when network infrastructure becomes a matter of both economic dependence and national security (Nocetti, 2023, p. 21).

The geopolitical dimensions of 5G have emerged through the debate over Chinese telecommunications equipment manufacturers, particularly Huawei and ZTE. The US campaign against Huawei, beginning in 2019, sought to exclude the company from global 5G networks on security grounds. This campaign has had significant effects on European member states, which face difficult choices between security considerations, economic interests, and diplomatic relationships (Nardon, 2021).

Previously, Europe's digital ambitions were limited to the expansion of American tech giants; now, however, these ambitions have broadened to include China alongside the United States. These factors fuel a number of challenges for the European

Union and raise questions about its relationship with economic globalisation, which relies on China's production capacity, as well as the 'geopolitical' nature of the Commission, as evidenced since its establishment in December 2019 against a backdrop of transatlantic tensions. Thus, the 5G issue has so far highlighted a lack of cohesion within Europe in its dealings with China under Xi Jinping's leadership. Amid varying assessments across the continent, the competition between China and the United States reflects the difficulty Europeans face in defining their commercial and strategic position vis-à-vis China – and vis-à-vis the United States – at a time when the “technological nationalism” that Beijing seeks to export appears clearly defined. (N., pp. 193–254)

The European Union's capacity to act in the technological sphere, which is often overlooked in discussions, could be the beginning and end of a 'dynamic' strategy for the Old Continent in the field of 5G. This is a perspective that is beginning to emerge within the European executive, which, by identifying its critical dependencies in sectors considered strategic for Europe, is seeking to put measures in place to protect European interests. In other words, it is better to defend the European Union's 'technological sovereignty' through a careful assessment of Member States' critical dependencies before taking targeted action, whilst maintaining openness to the world, rather than adopting a traditional approach to sovereignty that masks the logic of mutual dependence which remains its defining feature. (fiott d. & theodosopoulos v, 2020, pp. 1–2.)

5. Europe's response to the 'Splinternet': the fear of Balkanisation

Sovereign policies have been the subject of ongoing international debate for many years, given their direct impact on the internet, the digital sphere as a whole, and emerging technologies (artificial intelligence, 5G networks, quantum computing). Much of this debate centres on the concept of 'fragmentation' or the 'Splinternet', which describes the disintegration of the unified global network under the influence of national sovereign policies, in direct contrast to the founding vision of the internet, which envisaged it as an open, globally interconnected network. (Confronting reality in cyberspace: Foreign policy for a fragmented internet, independent task force, 2022, pp. 193–254.)

The concept of 'cyber-Balkanisation' constitutes one of the earliest theoretical warnings against excessive optimism regarding the digital global village. In their seminal 1997 study, Marshall Van Alstyne and Erik Brynjolfsson warned that the development of a global communications infrastructure might not lead to the unification of societies, but rather to their fragmentation within 'cyber-Balkanisation' — that is, isolated digital spaces that are ideologically and identitarian homogeneous. (Van Alstyne, 1997, p. 1) This argument was later reinforced by the work of Cass Sunstein and Eli Pariser, who demonstrated that digital algorithms contribute to the perpetuation of 'echo chambers' (Cass R. Sunstein, 2017, pp. 59–72) and 'filter bubbles' (Eli Pariser, 2011, pp. 9–12), thereby reducing intellectual pluralism within the digital space.

However, this socio-sociological conception of fragmentation has not remained confined to the analysis of user behaviour, but has evolved to take on a structural and geopolitical dimension with the rise of digital sovereignty policies. In this context, Milton Mueller demonstrates that the prospects of the “disintegration of the internet” are primarily linked to states’ attempts to re-subjugate cyberspace to the logic of territorial sovereignty, through regulatory and technical tools such as data localisation, censorship, and the construction of closed national infrastructures. (Milton Mueller, 2017, p. 63.) This analysis confirms the findings of reports by the Organisation for Economic Co-operation and Development (OECD) and Freedom House, which point to increasing restrictions on data flows and a rise in the level of digital censorship globally, reflecting the transition of the internet from an open space to multiple spaces subject to divergent national policies. (Freedom House, 2024, pp. 28–35.)

In this context, the Balkanisation of cyberspace is no longer merely a side effect of technological development, but has become an expression of profound shifts in the structure of the international system, where major powers compete to impose their models of internet governance. Anupam Chander has described this phenomenon using the concept of the ‘Splinternet’, which refers to the division of the internet into distinct digital blocs or islands that reflect existing geopolitical divisions. (Chander, 2019, pp. 1671–1698.) Accordingly, it can be argued that the fragmentation of cyberspace today represents one of the most prominent

manifestations of the transition from open digital globalisation to a fragmented digital system, in which technical considerations intersect with issues of sovereignty, security and power.

In this context, the European strategy for digital sovereignty is based on a normative vision that seeks to reconcile the requirements of technological independence with the preservation of the global and open nature of the internet. In this framework, the European Union has adopted the concept of ‘Open Strategic Autonomy’, which aims to reduce technological dependence on external actors without retreating into a model of digital isolation or contributing to the dismantling of the global network. In its document ‘Shaping Europe’s Digital Future’, the European Commission has emphasised that the strategic objective is to ‘strengthen Europe’s ability to control its digital infrastructure and data, whilst maintaining an open and globally interconnected digital economy. In doing so, Europe is positioning itself as an actor seeking to reshape digital globalisation rather than withdraw from it. (European Commission, 19 February 2020, p. 3.)

The implementation of this vision relies on a forward-looking legal approach, which is one of the key features of the European strategy. The General Data Protection Regulation (GDPR) forms the cornerstone of this strategy, enshrining the principle of ‘data sovereignty’ and imposing strict rules on the processing of personal data, with a clear extraterritorial impact extending to non-European companies (Regulation (EU) 2016/679, Art. 3). The Digital Services Act and the Digital Markets Act

complement this approach, with the former aiming to regulate digital content and combat disinformation, whilst the latter seeks to limit the dominance of large digital companies (Gatekeepers) and ensure fair competition within the European market (Regulation (EU) 2022/2065; Regulation (EU) 2022/1925). Thus, the European Union has transformed from a traditional economic actor into a normative regulatory power using the law to reshape the digital space. (European Parliament and Council of the European Union, 2022, p. 30.)

This approach takes on a clear geopolitical dimension in the context of the competition between the American and Chinese models. The European Union seeks to impose a third model based on values-based regulation. Anu Bradford has highlighted this trend through the concept of the 'Brussels Effect', which refers to Europe's ability to export its regulatory standards globally thanks to the size of its internal market and its economic strength (Bradford, 2020, p. 30). The GDPR is now a global benchmark emulated in many national legislations, reflecting the EU's transformation into an influential actor in international internet governance (Anu Bradford, 2020)

However, this strategy reveals a profound structural paradox. Whilst the European Union supports the principle of 'free flow of data with trust' promoted by the Organisation for Economic Co-operation and Development (OECD, 2021), its strict data protection rules and restrictions on data transfers outside European borders create regulatory digital borders. Milton Mueller argues that the multiplicity of legal and regional regimes may lead to what is termed 'regulatory fragmentation', where

fragmentation occurs not because of technology, but as a result of differing legal rules. Consequently, the European strategy, despite its integrative nature, may indirectly contribute to deepening the Balkanisation of cyberspace rather than countering it. (Milton Mueller, 2017, p. 63.)

6. CONCLUSION

This study demonstrates that the European Union's strategy on digital sovereignty cannot be understood merely as a circumstantial response to shifts in the geopolitical landscape, but rather as an expression of a profound structural paradox that characterises the reshaping of the global digital order. On the one hand, the European Union seeks to establish a liberal digital model based on openness, interoperability and the protection of rights and freedoms; on the other hand, it imposes the adoption of centralised regulatory and security tools to counter the phenomenon of geopolitical 'weaponisation of dependencies', leading to the reproduction of a logic of control within a space that was supposed to be borderless.

This paradox does not represent a temporary anomaly, but rather constitutes a structural feature of the European approach. Analyses have shown that the legal instruments adopted by the Union — notably the General Data Protection Regulation (GDPR), the Digital Services Act (DSA) and the Digital Markets Act (DMA) — have contributed to strengthening its regulatory sovereignty and transforming it into a global normative power, in what is known as the 'Brussels effect'. However, this regulatory reach, supported by the role of institutions such as the European Commission and the Court of

Justice of the European Union, has simultaneously led to the creation of legal digital borders by imposing extraterritorial standards, thereby reinforcing the dynamics of ‘regulatory fragmentation’ at the global level.

On this basis, the study shows that European digital sovereignty is no longer merely a tool for protecting the digital space, but has become an active factor in reshaping its structure, including by contributing – indirectly – to the deepening of the ‘Splinternet’ phenomenon. This is clearly illustrated by the case study of 5G, which revealed the difficulty of achieving a stable balance between the requirements of strategic independence and the logic of interdependence, whilst also highlighting the limits of European cohesion in the face of geopolitical competition between major powers.

In this context, a broader interpretation could be proposed, namely that digital sovereignty, in its contemporary form, no longer merely conflicts with the logic of digital globalisation, but has become one of the structural factors reshaping it, even if this is at the expense of its unity. Hence, the European model presents itself as an attempt to establish ‘open digital sovereignty’, seeking to reconcile the requirements of protection and openness; however, the success of this model remains contingent upon its ability to limit its unintended consequences in reinforcing fragmentation.

Looking ahead, three possible trajectories can be envisaged:

First, the continuation of the ‘regulated openness’ model, which attempts to reconcile sovereignty and integration;

Second, the escalation of digital fragmentation dynamics towards a multi-bloc system;

Third, the emergence of an international consensus model that reorganises data flows within a common legal framework.

However, the likelihood of any of these scenarios will remain linked to the evolution of geopolitical balances and the extent to which international actors are able to move beyond a logic of conflict towards a logic of shared governance.

Finally, the study concludes that the European Union’s commitment to digital sovereignty goes beyond merely achieving technological independence, raising a deeper question regarding the possibility of redefining the rules of the global digital system without compromising the liberal foundations upon which it was built. Consequently, the real challenge lies not in achieving sovereignty per se, but in the ability to exercise it without it becoming a tool for reproducing divisions within the global digital space.

In light of the above, a set of academic recommendations is advanced, grounded in the argument that the pursuit of digital sovereignty, as currently framed, risks reinforcing the very fragmentation it seeks to counter. This underscores the need to develop a balanced conception of digital sovereignty that reconciles openness with regulatory safeguards, rather than translating interdependence into mechanisms of control. It also calls for a critical reassessment of the cumulative effects of legal frameworks in producing forms of regulatory fragmentation (Splinternet), as well as a rethinking of strategic autonomy in light of structurally

embedded interdependence. Ultimately, strengthening international digital governance mechanisms appears not as a complementary option, but as a necessary condition to prevent the progressive reconfiguration of the digital space into competing and fragmented spheres.

7. Bibliography List:

1. Bradford, A. (2020), *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, New York, USA.
2. Farrell, H. & Newman, A. L. (2024), *Underground Empire: How America Weaponized the World Economy*, Henry Holt and Company, New York, USA.
3. Mueller, M. (2017), *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Polity Press, Cambridge, UK.
4. Pariser, E. (2011), *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Press, New York, USA.
5. Sunstein, C. R. (2017), *Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton, USA.
6. [Author not specified] (n.d.), *The Great Decoupling: China, America, and the Struggle for Technological Supremacy*, Hurst.
7. Chander, A. (2019), "The Splinternet", *Georgetown Law Journal*, Vol. 107, No. 6.
8. Colbert, C. (2026), "Réguler pour exister : la souveraineté numérique européenne comme stratégie géopolitique face à la domination des plateformes", *Regards géopolitiques*, Vol. 12, No. 4.
9. Farrell, H. & Newman, A. L. (2019), "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", *International Security*, Vol. 44, No. 1.
10. Nardon, L. (2021), "États-Unis/Europe : sept enjeux du numérique", *Institut français des relations internationales*.
11. Lee, J. (2025), "What Is Digital Sovereignty?", *Trend Micro*, 9 December 2025.
12. Nocetti, J. (2021), "L'Europe reste-t-elle une colonie numérique des États-Unis ?", *Politique étrangère*, No. 3.
13. Nocetti, J. (2023), "La souveraineté numérique : dix ans de débats, et après ?", *Enjeux numériques*, No. 23.
14. Nocetti, J. (2024), "Digital Sovereignty in the MENA Region: Overcoming Paradoxes to Ensure Digital Resilience", *Euromesco Policy Study*, No. 36.
15. Nye, J. S. (2015), "Contest and Conquest: Russia and Global Internet Governance", *International Affairs*, Vol. 91, No. 1.
16. CIGREF (2024), *Rapport d'orientation stratégique*, CIGREF, Paris, (consulted on 29/08/2026).

17. European Commission (2020), État de l'Union 2020 : La Commission von der Leyen – Bilan de la première année, (consulted on 29/08/2026).
18. European Commission (2020), Shaping Europe's Digital Future, COM (2020) 67 final, Brussels, 19 February 2020.
19. Fick, N., Miscik, J., Segal, A. & Goldstein, G. M. (2022), Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet, Independent Task Force Report No. 80, Council on Foreign Relations, (consulted on 29/08/2026).
20. Fiott, D. & Theodosopoulos, V. (2020), Sovereignty over Supply? The EU's Ability to Manage Critical Dependencies While Engaging with the World, EUISS Brief No. 21, European Union Institute for Security Studies, Paris.
21. Freedom House (2024), Freedom on the Net 2024: The Repressive Power of Artificial Intelligence, Freedom House, Washington, DC.
22. Lee, J. (2025), "What Is Digital Sovereignty?", Trend Micro, 9 December 2025, (consulted on 29/08/2026).
23. Nardon, L. & [co-author not specified] (2021), États-Unis/Europe : sept enjeux du numérique, Institut français des relations internationales, (consulted on 29/08/2026).
24. Pomfret, J. & [co-author not specified] (2024), "Exclusive: Illicit Chip Flows to Russia Seen Slowing, but China, Hong Kong Remain Transshipment Hubs", Reuters, 22 July 2024, (consulted on 29/08/2026).
25. Thys, R. (2022), "La Russie se retrouve tenue à l'écart des processeurs les plus avancés", Numerama, 9 May 2022, (consulted on 29/08/2026).
26. [Author not specified] (2021), "China's Microchip Ambitions: Semiconductors Advance the Next Phase of Technonationalism", (consulted on 29/08/2026).
27. [Author not specified] (2023), "China Invested US\$290.8 Billion in Semiconductor Projects Between 2021–2022", DigiTimes Asia, Taipei, 27 June 2023, (consulted on 29/08/2026).
28. European Parliament & Council of the European Union (2022), Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).