This is an Accepted Manuscript of Victor Henriquez Diaz and Edoardo Celeste, 'EU AI Policies and the Price of Digital Sovereignty: Between Open Strategic Autonomy and Protectionist Effects', in Olivier Delas et al (eds), L'Espace transatlantique à l'épreuve du numérique global (Larcier 2025), 353-382, https://www.larcier-intersentia.com/fr/l-espace-transatlantique-l-epreuve-numerique-global-9782802776598.html#product.info.tab.details

EU AI Policies and the Price of Digital Sovereignty: Between Open Strategic Autonomy and Protectionist Effects

Victor Henriquez Diaz

PhD Researcher, Dublin City University, Ireland

Edoardo Celeste

Associate Professor of Law, Technology and Innovation

Dublin City University, Ireland

I. Introduction

The EU digital economy is increasingly dependent on third countries. US digital services and Chinese digital goods see little local competition[1]. For its first decades of existence, the EU digital agenda exclusively aimed to foster the introduction and use of digital technologies both in the public and in the private sectors. More recently, a new principle has emerged to guide the EU digital transition: digital sovereignty.

There is no univocal definition of digital sovereignty, but, as will be further explained below, it can be generally described as the capacity to control all the elements of a country's digitalisation strategies without being dependent on foreign actors. The EU is increasingly referring to the need to preserve digital sovereignty while developing its digital policy and, in this context, a central role is played by the regulation of Artificial Intelligence (AI). AI is relevant for the EU in a broad variety of policy areas, from the green transition to the military, from the digitalisation of public administration to research and development. Despite an increased attention at Union and member state level, the US and China remain the undiscussed leaders in the AI sector. The EU cannot compete against these two 'technopoles', but, as shown

[1] M. MAYER AND Y. LU, «Digital Autonomy? Measuring the Global Digital Dependence Structure», (2022) Center for Advanced Security, Strategic and Integration Studies, online: <https://digitaldependence.eu/wp-content/uploads/2022/05/DDI_Paper.pdf>.

in the past, it can leverage its centrality in international trade relations to influence foreign standards.

The Union does so by exercising its normative power on a global plane[2]. The EU has been the first jurisdiction to adopt a coherent set of rules to guide and limit the development of AI, in this way setting a standard for the rest of the world. By imposing stricter requirements for AI, the EU aims to preserve its digital sovereignty vis-à-vis foreign players. This represents a key component of a broader strategy seeking to foster the 'open strategic autonomy' of the Union, defined as its capacity to be 'as open as possible and as autonomous as necessary' in key commercial fields[3]. Yet, at the same time, these stringent requirements can be seen as trade barriers and lead to allegations of protectionism. Indeed, non-EU actors are disadvantaged by high compliance costs as well as by tariffs and subsidies supporting local players.

Neither the relationship between EU AI policy and digital sovereignty strategies nor its economic effects are apparent. There is no single policy document or academic work reconstructing this link in an explicit and coherent way. This chapter aims to fill this gap by critically analysing how the EU AI policy contributes to achieve digital sovereignty objectives, looking in particular at its economic effects. The paper will be articulated into two logical parts: the first one (sections II and III) aims to understand to what extent the principle of digital sovereignty is driving the development of EU AI policies, while the second one (sections IV and V) investigates and contextualises the economic effects of this pairing.

Section II will retrace the origins of digital sovereignty ambitions within the EU, highlighting its economic and geopolitical drivers as well as clarifying its relationship with the concept of 'open strategic autonomy'. Section III will examine to what extent the components of EU AI policy contribute to digital sovereignty objectives. To this end, we will distinguish between 'centrifugal' and 'centripetal' policies. The first ones rely on the EU normative power to extend standards beyond its borders, while the second ones seek to reshore physical components of the digitalisation process within the EU.

Section IV will analyse the economic effects of EU AI policies inspired by the principle of digital sovereignty. We will identify the emergence of both increasing costs of compliance as

[2] See the scholarship on the concept of European 'normative power': see ex multis I. MANNERS, « Normative Power Europe: A Contradiction in Terms? » (2002) 40: 2, *Journal of common market studies*, at 235; and the studies on the so-called 'Brussels effect': see ex multis A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford, Oxford University Press, 2020.

[3] See L. SCHMITZ AND T. SEIDL, «As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy» (2023) 61:3, *Journal of Common Market Studies*, at 834.

well as access barriers for non-EU actors, respectively due to the introduction of stricter regulatory requirements, on the one hand, and subsidies and tariffs, on the other hand. Section V will finally discuss whether we could then possibly speak of phenomenon of 'digital protectionism' associated with EU AI policies. In order to do so, we will propose a broader interpretation of digital protectionism, enlarging the current scholarly definition. We will however conclude that digital protectionism in the EU AI sector is qualified by a relative openness due to recently emerged geopolitical circumstances that require a strategic form of multilateralism.

II. European digital sovereignty and strategic autonomy

A. The emergence of EU digital sovereignty ambitions

Despite it becoming a popular term in policy discourses around the globe, there is no univocal definition of digital sovereignty neither in academia nor in policy documents[4]. It represents a novel application of the traditional concept of sovereignty, whose difficult theorisation might be sufficient to justify the lack of consensus related to its application in the digital context[5].

The concept of digital sovereignty possesses at least two main, mutually complementing facets. On the one hand, digital sovereignty is an expression of self-determination. From this perspective, it can be understood as the capability of states to act autonomously in relation to digital resources and technologies, according to their values and interests as well as for their benefit[6]. Following this approach, digital sovereignty represents a tool to reinforce authority and control over the whole digital sphere, ranging from digital infrastructure to data, to better protect citizens from the emerging challenges generated by new technologies[7]. A second and

[4] See E. CELESTE, «Digital Sovereignty in the EU: Challenges and Future Perspectives» in F. FABBRINI, E. CELESTE AND J. QUINN (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart publishing, 2021.

[5] See H. KALMO AND Q. SKINNER (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept,* Cambridge, Cambridge University Press, 2010.

[6] See M. BRAUN AND P. HUMMEL, «Is Digital Sovereignty Normatively Desirable?» (2024) *Information, Communication & Society*, at 1–14; J. POHLE «Digital sovereignty. A new key concept of digital policy in Germany and Europe» (2021), online: <https://www.transcript-verlag.de/978-3-8376-5760-9/practicing-sovereignty/>; M. ROBLES-CARRILLO, «Sovereignty vs. Digital Sovereignty», (2023) 1: 3, *Journal of Digital Technologies and Law*, at 673–690.

[7] See F. MUSIANI, «Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices» (2022) 25 I*nformation, Communication & Society*, at 785; G.

complementary aspect of digital sovereignty is expression of a need of independence from third actors. In this sense, it would revolve around developing and preserving autonomy from other countries and limiting the level of external dependencies from foreign critical technologies[8]. Here, it is also possible to read digital sovereignty through the lens of competitiveness. It would be conceived as the capacity to determine and maintain a nation's -or region's- model in the digital sector in competition with other players, rather than a siloed governance model disconnected from any external influence[9].

Irrespective of its academic definition, digital sovereignty is a concept that has first populated the political discourse[10], particularly within the European Union. During her first term, European Commission president Von der Leyen introduced digital sovereignty as the "capability that Europe must have to make its own choices, based on its own values, respecting its own rules.[11]" Digital sovereignty is one of the EU paths to conquer a suitable level of strategic autonomy and digital independence[12]. The rationale behind such autonomy and independence is embedding and upholding the European fundamental values in the digital realm. Therefore, without such degree of independence, the effective defence of fundamental values cannot be guaranteed. In fact, the EU Declaration of Digital Rights and Principles adopted in 2022 acknowledged the importance of digital sovereignty to achieve the digital transformation[13].

The main drivers of the EU digital sovereignty strategy are the EU's external dependence and current geopolitical tensions. Both aspects have been exacerbated after the COVID-19

FALKNER AND OTHERS, «Digital Sovereignty - Rhetoric and Reality» (2024) 31: 8, *Journal of European Public Policy,* at 2099.

[8] SERENELLA CARAVELLA AND OTHERS, «Technological Sovereignty and Strategic Dependencies: The Case of the Photovoltaic Supply Chain» (2024) 434 *Journal of Cleaner Production*, 140222.

[9] D. INNERARITY, «European Digital Sovereignty» (2021) IED Strategic Research Paper, at 6, online: <https://www.iedonline.eu/download/2021/IED-Research-Paper-Innerarity.pdf >.

[10] J. POHLE AND T. THIEL, «Digital Sovereignty» (2020) 9: 4, *Internet Policy Review*, at 2.

[11] EUROPEAN COMMISSION, 'Op-ed by Commission President von der Leyen' (*European Commission - Press Corner*, 19 February 2020), online: <https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260> [Accessed 20 January 2025].

[12] T. CHRISTAKIS, *«* "European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy», Social Science Research Network, (7 December 2020), at 11, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098>.

[13] Recital 6. See E. CELESTE, «Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights» in ANNEGRET ENGEL, XAVIER GROUSSOT AND GUNNAR THOR PETURSSON (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights*, Springer, 2024; E. CELESTE, V. HENRIQUEZ DIAZ AND E. MACHADO NETO, «Digital sovereignty in an 'open manner'? EU tensions between autonomy and competitiveness» in *The governance of digital trade: crossroads of divergent approaches* (Laval University Press, forthcoming).

pandemic, when countries realised how much they relied on other nations' products[14]. Mayer and Lu highlighted concerning levels of interdependencies between nations in the digital sector[15]. Their Digital Dependence Index reveals the extent to which some European countries rely on foreign technologies, thus intensifying their levels of vulnerability[16]. In contrast, the Index shows that countries like China, South Korea, Russia, Kenya and the US have increased their autonomy levels in the last decade[17].

Such "excessive reliance" on digital services, infrastructure and components is a pressing matter because it could potentially affect critical sectors of daily operations for Member States[18]. These concerns extend also to EU businesses, a considerable number of which run their activities based on alliances with non-EU actors ranging from electronic communications to supply industry[19]. Such a dependence on a small number of suppliers is also subject to the risk of market disruptions, should the partnership fail or be affected by unforeseen events[20].

Due to these concerns, the guiding principle of the EU digital strategy is not only to diversify global alliances, as it is nevertheless necessary[21], but also to achieve a minimum level of autarchy in the field. It is not interdependency what matters most, but from whom. As explained by Monsees and Lambach, the European approach to digital sovereignty is heavily influenced by geopolitical objectives, aiming to affirm the Union's leadership vis-à-vis other international actors[22]. Indeed, under the shield of digital sovereignty, the EU aims at building a stronger

[14] J. THUMFART, «The Norm Development of Digital Sovereignty between China, Russia, the EU and the US: From the Late 1990s to the Covid-Crisis 2020/21 as Catalytic Event» in D. HALLINAN, R. LEENES, P. DE HERT (eds), *Data Protection and Privacy: Enforcing Rights in a Changing World*, (2021); see also H. ROBERTS AND OTHERS, «Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies» (2021) 10: 3, *Internet Policy Review*.

[15] M. MAYER AND Y. LU, «Digital Autonomy? Measuring the Global Digital Dependence Structure», op. cit., at 2.

[16]Center for Advanced Security, Strategic and Integration Studies (CASSIS) Universität Bonn, «Vermessung Der Digitalen Dependenz' (*Digital Dependence Index*)», online: <https://digitaldependence.eu/en/> [Accessed 20 January 2025].

[17] MAYER AND LU, «Digital Autonomy? Measuring the Global Digital Dependence Structure», *op. cit.,* at 7.

[18] T. CHRISTAKIS, « "European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy », *op. cit.,* at 45.

[19] EUROPEAN COMMISSION, Communication «White Paper: How to master Europe's digital infrastructure needs? » COM (2024) 81 final, online: <https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs> [Accessed 27 March 2024].

[20] *Ibid*.

[21] M. DRAGHI, «The Future of European Competitiveness Part A», 3, 13, online: <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en>.

[22] L. MONSEES AND D. LAMBACH, «Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity» (2022) 31 3 *European Security*, at 377.

position that balances the defence of democratic principles and human rights while fostering economic competitiveness.

It is easier to understand the meaning of digital sovereignty by placing it in the context of trade frictions around the world. For instance, since 2017 there has been an apparent and increasing rivalry in the tech sector between the US and China[23]. Both countries have been called out for assuming techno-nationalist perspectives with the aim of achieving digital self-sufficiency, overcoming supply chain vulnerabilities and driving out foreign competitors[24]. The effect of this cold war 2.0 affects also bilateral trade[25]. Both countries have resorted to tariffs, local content requirements, tax incentives and capital incentives provided that there are no links with a foreign competitor[26].

Technology is a new field to measure political power and ideologies. Contending views on rights, freedom and democracy between countries such as the US, Russia and Iran, which have permeated into the digital realm, pressure the EU to rethink its position in the digital world[27].

Against this backdrop, digital sovereignty is presented as the required and necessary approach of the EU to achieve a more competitive, resilient and secure position within the digital field. Therefore, the concept goes beyond political discourse. It has a normative component rooted in self-determination with tangible legal consequences that can be seen in the current EU digital regulatory and policymaking landscape, as it will be discussed in the following sections[28]. Thus, digital sovereignty allows the EU and Member States not only to reinforce their control over the digital field, but to insert the European value-based model into the development of new technologies.

---

[23] «Understanding the US-China Tech War», South China Morning Post, (31 March 2024), online: <https://www.scmp.com/knowledge/topics/us-china-tech-war-rivalry/news> [Accessed 31 March 2024].

[24] P. EVANS, «Techno-nationalism in China–US Relations: Implications for Universities» (2020) 12: 2 *East Asian Policy* at 81 ; see also V. MISHRA, «The Great U.S.-China Tech Decoupling: Perils of Techno-Nationalism», *Observer Research Foundation*, (2023), online: <https://www.orfonline.org/expert-speak/the-great-u-s-china-tech-decoupling/> [Accessed 04 November 2023].

[25] A. CAPRI, «US-China Decoupling in Tech », *Hinrich Foundation*, (4 June 2020), online: <https://www.hinrichfoundation.com/research/wp/tech/us-china-decoupling-tech/> [Accessed 20 January 2025].

[26] E. CELESTE, V. HENRIQUEZ DIAZ AND E. MACHADO NETO, « Digital sovereignty in an 'open manner'? EU tensions between autonomy and competitiveness », *op. cit*.

[27] C. MARTIN, «Geopolitics and Digital Sovereignty» in H. WERTHNER AND OTHERS (eds) in *Perspectives on Digital Humanism*, Springer International Publishing, 2022.

[28] G. GORDON, «Digital Sovereignty, Digital Infrastructures, and Quantum Horizons» (2024) 39 *AI & SOCIETY*, at 125.

B. No sufficiency without alliance: open strategic autonomy

Digital sovereignty is not an isolated conception; it is often accompanied by references to the notion of 'strategic autonomy'[29]. These concepts have a symbiotic and instrumental relation. Strategic autonomy originated in the field of security and defence and was progressively applied to other key EU policy areas, such as trade and technology[30]. It is understood as the "capacity to act autonomously when and where necessary and with partners wherever possible"[31]. Tocci defines it as the ability of nations to live according to their own values through the preservation of their internal rules while actively participating at the international level[32].

In 2020, the EU Commission adopted the communication 'Shaping Europe's Digital Future'. The document introduced the concept of 'technological sovereignty' as 'Europe's ability to define its own rules and values in the digital age' that would rely on the EU's autonomous development and on the strengthening of local digital capacities to reduce dependence on other global players[33]. The essential role of strategic autonomy to secure full control on digital assets became apparent. The document highlights that this approach does not aim to penalise any international actors but prioritizes Europeans' needs and values[34].

The implementation of strategic autonomy in these new policy areas triggered a requalification of the concept. The EU Trade Policy Review 2021 coined the term of '*open* strategic autonomy' to denote the effort to balance cooperation opportunities with the necessity to act autonomously[35]. Open strategic autonomy does not mean excluding cooperation, but rather

---

[29] M. TAMBIAMA, «Digital Sovereignty for Europe», online: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf> [Accessed 15 November 2024].

[30] G. KÜBEK AND I. MANCINI, « EU Trade Policy between Constitutional Openness and Strategic Autonomy » (2023) 19 :, *European Constitutional Law Review*, at 518 ; D. BROEDERS, F. CRISTIANO AND M. KAMINSKA, « In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions » (2023) 61 :, *Journal of Common Market Studies*, at 1261.

[31] G. KÜBEK AND I. MANCINI, «EU Trade Policy between Constitutional Openness and Strategic Autonomy», *op. cit.*; see also M. DAMEN, «EU Strategic Autonomy 2013-2023: From Concept to Capacity», online: <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589> [Accessed 20 January 2025].

[32] N. TOCCI, « European Strategic Autonomy: What It Is, Why We Need It, How to Achieve It » (2021), *IAI Istituto Affari Internazionali*, online: <https://www.iai.it/en/pubblicazioni/c09/european-strategic-autonomy-what-it-why-we-need-it-how-achieve-it> [Accessed 7 August 2024].

[33] UE, European Commission, Communication *Shaping Europe's Digital Future*, COM (2020) 67 final, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067> [Accessed 20 January 2025].

[34] *Ibid.*

[35] G. KÜBEK AND I. MANCINI, «EU Trade Policy between Constitutional Openness and Strategic Autonomy», *op. cit.,* at 521.

fostering collaboration with selected partners[36]. The adjective 'open' implies a willingness to comply with the multilateral system, preserving European standards and protecting the EU when collaboration with third countries becomes risky[37]. It is a convenience-based and flexible cooperation model. Nonetheless, relations are to be built excluding current and potential overreliance on external actors.

Open strategic autonomy has an economic focus. As suggested by Mariotti, it gives a central role to industrial policies that protect national industries against foreign competition with interventionist actions, thus departing from traditional multilateralism[38]. Assuming open strategic autonomy as a European goal has impacted the digital field, the quest for digital sovereignty combined with open strategic autonomy has led the EU to adopt a particular regulatory and policy making scheme to guarantee European industrial tech development. The following section discusses the influence of the principles of digital sovereignty and open strategic autonomy on the EU AI strategy.

III. A two-sided strategy: Centripetal and centrifugal approaches

A particular challenge posed by the digital ecosystem lies in its partially immaterial nature. This has challenged the ability of countries to control technology within their territorial boundaries[39]. The hardware supporting a specific technology can have a physical location, but the information within it, such as data, can flow across multiple places at incredible speed.

In light of this twofold nature of digital technology, at the same time territorially rooted and transnational, the EU digital sovereignty strategies have adopted two complementary approaches[40]. On the one hand, the EU aims at reinforcing its digital sovereignty in a 'centripetal' way[41]. This is done through policies and regulations that call back or reattract

[36] A. GARCÍA HIGUERA AND C. WEICHERT, «What If Open Strategic Autonomy Could Break the Cycle of Recurring Crises?», online: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747420/EPRS_ATA(2023)747420_EN.pdf> [Accessed 2 August 2024].
[37] L. SCHMITZ AND T. SEIDL, «As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy», *op. cit.*
[38] S. MARIOTTI, « "Open Strategic Autonomy" as an Industrial Policy Compass for the EU Competitiveness and Growth: The Good, the Bad, or the Ugly? » (2024) 14 *Journal of Industrial and Business Economics*, at 19.
[39] See E. CELESTE, «Brexit and the Risks of Digital Sovereignism» in E. CELESTE AND OTHERS (eds), *Data Protection and Digital Sovereignty Post-Brexit*, Hart, 2023.
[40] See E. CELESTE, « Digital Sovereignty in the EU: Challenges and Future Perspectives », *op. cit.*; E. CELESTE, «Brexit and the Risks of Digital Sovereignism», *op. cit*.
[41] E. CELESTE, «Digital Sovereignty in the EU: Challenges and Future Perspectives », *op. cit.*

digital technologies and infrastructures within EU borders. Not only does this strategy enhance the possibility to regulate and control digital technologies, but also fosters the local development of digital products, services and infrastructure[42]. An apparent example is represented by the European Chips Act, which aims at supporting semiconductor local industries in order to safeguard the stability of the supply chain. In a nutshell, it is all about strengthening the EU digital capabilities and resilience within its own territory.

On the other hand, a 'centrifugal' mechanism has also been adopted by the EU through the extension of its regulatory reach beyond the bloc's territorial boundaries[43]. The global and virtual nature of the digital ecosystem makes it impossible for the EU to create an autonomous and independent digital cluster made in and for the EU. There are goods and services that businesses from third countries will continue to supply to the EU. For this reason, the EU has no other choice than to rely on its normative power, by attempting to spread its values and standards as much as possible beyond its borders. In this context, phenomena like the extraterritoriality of the GDPR or the so-called Brussels effect, generated by EU digital regulation, have been the most studied by the existing scholarship[44]. More recently, the Digital Services Act implemented the same extraterritorial formula of the GDPR, by applying to recipients of services located in the EU, despite the service providers' place of establishment[45]. A dynamic also followed by the Digital Markets Act, which establishes new rules for big online gatekeepers to ensure a fairer competition among providers of digital goods and services[46]. But interestingly, such a centrifugal regulatory approach also made its way through European soft law with the Declaration of European Digital Rights and Principles, which was adopted by the EU in 2023 in order to provide a comprehensive overview of EU core values for the digital transition[47].

---

[42] E. CELESTE, H. DIAZ AND M. NETO, « Digital sovereignty in an 'open manner'? EU tensions between autonomy and competitiveness », *op. cit.*

[43] E. CELESTE, «Digital Sovereignty in the EU: Challenges and Future Perspectives», *op. cit.*

[44] See, ex multis, C. KUNER, «Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law» (2015) 5:, *International Data Privacy Law*, at 235 ; F. FABBRINI AND E. CELESTE, «The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders » (2020) 21:, *German Law Journal*, at 55; A. BRADFORD, *Digital Empires: The Global Battle to Regulate Technology*, Oxford, *Oxford* University press, 2023.

[45] EU, *Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)* (Text with EEA relevance), [2022] OJ, L 277/1, article 2.

[46] EU, *Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)* (Text with EEA relevance), [2022] OJ, L 265/1, article 1.

[47] See E. CELESTE, «Brexit and the Risks of Digital Sovereignism», *op. cit*.

As will be explained in the next sections, this twofold approach adopted by the EU to advance its digital sovereignty ambitions shaped the current artificial intelligence strategy of the Union.

A. A tool for global influence: The AI Act

The EU AI Strategy was launched in 2018 to advance a coordinated approach at European level to the development of artificial intelligence for societal good[48]. It pivots on a core piece of regulation, the AI Act, and encompasses other "satellite" regulations and policies. Comprehensively regarded, these instruments aim to boost technological and industrial capacity, modernise education and training systems, and guarantee an adequate legal framework[49]. The concept of digital sovereignty is mentioned in some of the key components of this policy strategy, such as the EU Commission's proposal of the AI Act[50], but both policy and regulatory instruments as well as scholarly works have not so far provided a comprehensive reconstruction of how the EU AI strategy is contributing to achieve the EU digital sovereignty ambitions. The aim of this section is to start filling this gap. In order to do so, we will follow the conceptual categorisation of the regulatory approaches adopted in the context of the EU digital sovereignty strategy presented in the previous section, which distinguishes between a centripetal and a centrifugal model.

The AI Act was adopted on 13th June 2024 after a long legislative journey that started in 2021[51]. It is a comprehensive regulation that takes a horizontal approach to ensure that AI systems remain trustworthy, transparent and uphold EU fundamental rights and values from the phase of development to commercialisation[52]. Regulations in the EU have an immediate legally binding value and they do not require any transposition at the level of the member states. The

---

[48] UE, European Commission, *Artificial Intelligence for Europe*, Communication, COM (2018) 237 final, at 2, online: https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe>.
[49] *Ibid*, at 3.
[50] UE, European Commission, *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, COM (2021) 206 final, at 6, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206>.
[51] T. HICKMAN AND OTHERS, «Long Awaited EU AI Act Becomes Law after Publication in the EU's Official Journal», *White & Case LLP*, (16 July 2024) , online: <https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal> [Accessed 20 January 2025].
[52] J. LAUX, S. WACHTER AND B. MITTELSTADT, « Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk » (2024) 18 :, *Regulation & Governance,* 3, online: <https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12512> [Accessed 20 January 2025], at 1 ; UE, European Commission, 'AI Act', S*haping Europe's digital future*, (12 December 2024), online: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> [Accessed 21 July 2024].

new framework adopts an extraterritorial scope of application, in line with previous core pieces of EU digital law, such as the GDPR. Any AI-driven products, services or systems produced, imported or simply used within the EU will fall under the scope of the regulation[53].

The AI Act adopts a risk-based approach, which bans unacceptably high risks and introduces obligations for high and limited-risk systems[54]. The regulation allows manufacturers to evaluate the compatibility of their products with essential specified requirements alongside parameters determined by European standard-setting organisations, which can be mandated by the European Commission[55].

The adoption of the AI Act in June 2024 was propelled by the imminent end of the legislative term of the EU Parliament before the EU elections that took place in summer 2024. Approving this regulation before the start of the new legislature was a political imperative for the EU to exploit a first mover advantage. For a Union that, industrially and commercially speaking, lags behind the Unites States and China in the field of AI, it was of the utmost importance to play at least a regulatory role by becoming a global reference and source of inspiration for lawmakers around the world. It is here where the link between the AI Act and the digital sovereignty ambitions of the EU is fully apparent. In order to preserve its own values in a fast-moving market dominated by foreign players, the EU had to rely on its normative power and economic weight. This is an expression of what in the previous section we called 'centrifugal' approach. In the field of AI, the EU has limited possibilities to generate an industrial boom and be suddenly able to compete against the other global 'technopoles'. Hence, the need emerges to exploit its regulatory power and to spread its standards, following a centrifugal movement, from the Union to third countries.

While this was the only solution guaranteeing an immediate reaction to the harsh competition exercised in the field of AI by the United States and China, the EU did not resort exclusively to its regulatory power, but, as we will see in the next section, also put in place a series of measures to reshore in the Union and boost as much as possible the consolidation of the EU AI industry made in the EU.

---

[53] EU, *Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)* (Text with EEA relevance), 2024, article 2.
[54] *Ibid*, recitals 26-27.
[55] J. LAUX, S. WACHTER AND B. MITTELSTADT, «Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act» (2024) 53 *Computer Law & Security Review*, 105957.

B. From Europe for Europe: Boosting local AI capabilities

Since the launch of the EU AI strategy, the Union has progressively taken steps to reduce its gap with foreign technological industry. We can observe a progressive shift towards reinforcing EU digital infrastructure, a concept encompassing software and hardware, which can be tracked back to the adoption of the so called 'Digital Compass' in 2021[56].

The EU AI strategy consists in a panoply of policies and measures to create and provide stability to the AI supply chain. As represented in figure 1 below, we can identify three core areas of intervention, which may be deemed the backbone for the EU AI venture and correspond to the essential layers of the AI supply chain: a) data, cloud and edge technologies, b) semiconductors, and c) supercomputers and AI factories.

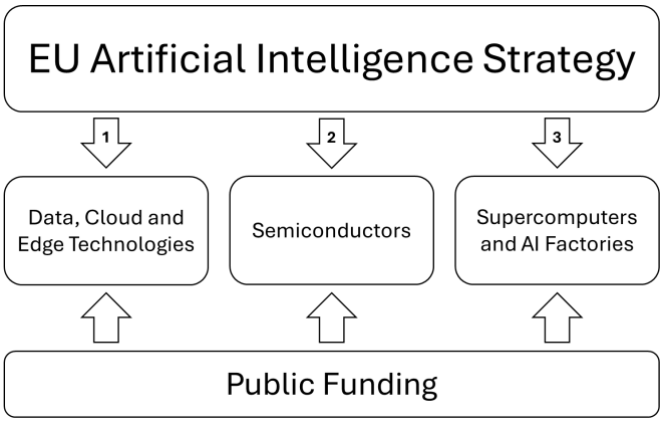

Figure 1: Core areas of intervention of the EU AI strategy in relation to the AI supply chain.

We will explore these three areas in the following sections, but it is important to anticipate that, from a financial perspective, they were all supported by a significant injection of EU funding, which relied on both ordinary and extraordinary budgetary measures. In the Multiannual Financial Framework 2021 – 2027 approved in December 2020, the portion allocated to innovation and digitalisation was of €132.8 billion, although this was reviewed again in 2024[57].

[56] UE, European Commission, «2030 Digital Compass: The European Way for the Digital Decade», Communication, COM (2021) 118 final; see also M. GORNET AND W. MAXWELL, «The European Approach to Regulating AI through Technical Standards» (2024) 13 *Internet Policy Review*, at 3.
[57] EU (Euratom), Council Regulation 2020/2093 of 17 December 2020 laying down the multiannual financial framework for the years 2021 to 2027 2020 (OJ, L LI 433/11).

This budget covered the expenses of the programmes Horizon Europe[58], Digital Europe[59], and InvestEU[60], whose aim is to foster EU competitiveness in the digital economy. Alongside these 'standard' tools, in the aftermath of the Covid-19 pandemic, the EU also established the Recovery and Resilience Facility as a temporary economic support instrument co-funded at Union and member state level[61]. The Facility, which is an essential component of the broader NextGenerationEU recovery plan, identified digitalisation as one of its priorities[62].

These funding programmes witness an increasing public participation into the digital sector. These initiatives have been labelled as a case of targeted resourcing, carried out by the Commission or, as in the case of the Recovery and Resilience Facility, by the Commission and Member States, to overcome the lack of funding provided by the market in the tech field[63]. Despite the fact that not all these funding instruments are exclusively dedicated to AI, they are key to support the EU AI strategy. For instance, while Digital Europe includes artificial intelligence as a specific objective[64], Horizon Europe and InvestEU have progressively deployed to support the development of SMEs working on AI[65].

1. Data, Cloud and Edge Technologies

Data has been a priority for the EU for over the past three decades. It has been considered the cornerstone of a successful transition towards the digital economy. Mastering data fuels the development of other technologies, which consequently raises productivity and

---

[58] EU, *Regulation 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013* (Text with EEA relevance), [2021] OJ, L170/1.

[59] EU, *Regulation 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240* (Text with EEA relevance), [2021] OJ, L166/1.

[60] «InvestEU Programme (2021–2027)» EUR-Lex, 3 May 2024, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4516649> [Accessed 20 January 2025], see also EU, *Regulation 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programme and amending Regulation (EU) 2015/1017*, [2021] OJ, L 107/30.

[61] EU, *Regulation 2023/435 of the European Parliament and of the Council of 27 February 2023 amending EU Regulation 2021/241 as regards REPowerEU chapters in recovery and resilience plans and amending EU Regulations No 1303/2013, (EU) 2021/1060 and (EU) 2021/1755, and Directive 2003/87/EC 2023*, OJ, L 63/1.

[62] See E. CELESTE AND G. DOMINIONI, « Digital and Green: Reconciling the EU Twin Transitions in Times of War and Energy Crisis » in F. FABBRINI AND C. PETIT (eds), *Research Handbook on Post-Pandemic EU Economic Governance & NGEU Law,* Edward Elgar, 2024.

[63] D. DI CARLO AND L. SCHMITZ, «Europe First? The Rise of EU Industrial Policy Promoting and Protecting the Single Market» (2023) 30 *Journal of European Public Policy*, at 2063.

[64] Regulation Digital Europe Programme, *op. cit.*, article 3(2)(b).

[65] Artificial Intelligence Act, *op. cit.,* recital 144; see also EU, European Commission, *Communication on Boosting Startups and Innovation in Trustworthy Artificial Intelligence*, 9.

efficiency. If at the origin, the EU regulatory intervention focused on personal data, the European Strategy for Data of 2020 broadened this horizon, by setting out the creation of Common European Data Spaces to guarantee the availability of data, the flow of data through different sectors and the respect of EU legal standards[66]. AI systems, indeed, rely on large language models that are fed by significant amount of data, which is not limited to personal data.

The European Data Space is expected to provide a pooling of interoperable resources that preserve privacy and security, allowing the processing and usage of data[67]. As part of the progress of the European Data Strategy, the EU adopted the Data Governance Act and the Data Act, which are two regulations that set rules to improve access, use and sharing of data[68]. Both instruments apply to businesses regardless of their place of establishment[69]. Thus, it consolidates the extraterritorial scope of application of EU law to non-EU companies, while harmonizing the legal framework of the EU data infrastructure.

In 2020, Member States signed the European Alliance for Industrial Data, Edge and Cloud, promising public investment in cloud technologies in light of the risks of long-term dependency on third party providers[70]. Notably, the inability to host data within the European Space and by European providers was reported as a main source of concern[71]. This is testified by the Terms of Reference of the Alliance, which highlight the vulnerabilities posed by the use of non-EU

---

[66] UE, European Commission, *A European strategy for data*, Communication, COM (2020) 66 final, at6, online: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data#:~:text=The%20strategy%20for%20data%20focuses,and%20societal%20progress%20in%20general>.

[67] UE, European Commission, *Common European Data Spaces*, Commission Staff Working Document, SWD (2022) 45 final, at 2, online: <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces>.

[68] EU, *Regulation 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending EU, Regulation 2017/2394 and EU, Directive 2020/1828 (Data Act)* (Text with EEA relevance), 2023 ; see also EU, *Regulation 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and EU, Directive 2020/1828 (Data Act)* (Text with EEA relevance), 2023.

[69] *Ibid*.

[70] UE, European Commission, *Declaration of the European Alliance for Industrial Data, Edge and Cloud*, 5 May 2021, online : <https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance> ; see also M. BAUER, F. ERIXON, AND D. PANDYA, « The EU's Trillion Dollar Gap in ICT and Cloud Computing Capacities: The Case for a New Approach to Cloud Policy » (2024), *European Centre for International Political Economy*, online : <https://ecipe.org/publications/eu-gap-ict-and-cloud-computing/#_ftn3> [Accessed 15 January 2025].

[71] A. MANGANELLI AND D. SCHNURR, «Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies», C*entre on Regulation in Europe*, February 2024, online: <https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf> [Accessed 10 November 2024].

providers[72]. Likewise, the aforementioned Declaration mentioned as objectives the "development and deployment of […] cloud and edge infrastructures and services"[73]. The EU aims to have up to 10.000 edge nodes deployed across the territory of its Member States by 2030[74]. By 2023, 1,186 edge nodes were already operational[75]. Edge computing aims to provide computing capability closer to end users in order to reduce the so-called 'latency', i.e. the reaction time, when relying on cloud infrastructure[76].

Overall, the EU is aware of the need to reduce internal fragmentation and external dependencies to fully harness the potential of data as a quintessential element to train AI models. AI innovation is presented by the EU Commission as one of the main ways to achieve digital sovereignty[77]. Such priority grows stronger and was recently confirmed by the EU Competitiveness Compass that highlighted the quintessential role of computing cloud and data infrastructures in the development of European AI[78].

2. Semiconductors

A second area that has been characterised by a high degree of intervention by the EU is represented by the semiconductor's industry. The EU Chips Act has been the vehicle to carry out a profound transformation of the sector with the goal of guaranteeing a safer and more resilient supply chain. The introduction of this regulation followed the adoption of the US CHIPS Act, a piece of legislation enacted to boost US semiconductor industry through subsidies, incentives and tax credits[79]. The US CHIPS Act has been controversial due to its open geopolitical purpose and the weaponization of the supply chain, not simply limiting its

[72] UE, European Commission, «Terms of Reference - European Alliance for Industrial Data, Edge and Cloud», at 2-3.
[73] *Ibid,* at 2.
[74] EU, *Decision 2022/2481 establishing the Digital Decade Policy Programme 2030*, [2022] OJ, L 323.4, article 4 (2)(c).
[75] UE, European Commission, *3rd Report - Edge Observatory for Digital Decade, Edge Computing Nodes: Characterization Deployment Monitoring and Trajectories – Study 2022.012*, June 2024, at 13.
[76] W. SHI AND OTHERS, «Edge Computing: Vision and Challenges» (2016) 3 *IEEE Internet of Things Journal*, at 637.
[77] *Ibid*, at 4; see also UE, European Commission, *Common European Data Spaces*, Commission Staff Working Document, SWD (2024) 21 final, at 4.
[78] UE, European Commission, *A Competitiveness Compass for the EU*, Communication, COM (2025) 30 final 5, at 6.6.
[79] United States, *Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act*, H.R. 4346, 2022 ; Y. LUO AND A. VAN ASSCHE, «The Rise of Techno-Geopolitical Uncertainty: Implications of the United States CHIPS and Science Act» (2023) 1:, *Journal of International Business Studies* , at 3; E. CELESTE, H. DIAZ AND M. NETO, «Digital sovereignty in an 'open manner'? EU tensions between autonomy and competitiveness», *op. cit.*

goals to the strengthening of the local industrial sector, but also aiming to weaken tech rivals like China[80]. It has represented a shift from the traditional laissez-faire trade policy to an industrial policy denoting a high level of State intervention[81].

The EU Chips Act introduced three main instruments: (i) the Chips for Europe Initiative; (ii) integrated production facilities and open EU foundries; and (iii) a coordination and mapping mechanism[82]. The Chips for Europe Initiative aims to bridge the existing gap between research and innovation as well as EU capacity-building in semiconductor technologies[83]. It is a way to take research into production, to operationalize knowledge in a business-oriented manner. The Initiative intends to improve the semiconductor value chain not only by constructing new capacities, but also by further developing existing ones[84]. In practice, it is implemented through a Joint Undertaking[85], which is constituted by initiatives promoted together by the EU, private entities and public bodies to advance research and innovation in the industrial sector, referred in the regulation as "institutionalised European partnerships"[86]. Only this pillar received more than a EUR 3 billion contribution through the EU-funding programmes Horizon Europe and Digital Europe[87].

Alongside the Initiative, the EU Chips Act also introduced the integrated production facilities and open foundries that are "locations" or "factories" made available for semiconductor manufacturing, production of relevant components for manufacturing or related processes[88]. They either work by offering their capabilities to other ventures or by integrating other stages of the semiconductor supply chain into their own business model[89]. An aspect worth commenting on in relation to this mechanism lies in the open embracement of a state aid model. In light of the public interest nature of the semiconductor industry, the regulation clearly mentions that "public support may be appropriate" and it shall be done according to EU law to

[80] LUO AND V. ASSCHE, «The Rise of Techno-Geopolitical Uncertainty: Implications of the United States CHIPS and Science Act», at 4.
[81] H. MA AND J. NING, «The Return of Protectionism: Prospects for Sino-US Trade Relations in the Wake of the Trade War» (2024) 4 *China Economic Quarterly International*, 182, at 26.
[82] EU Chips Act, article 1.
[83] *Ibid*, recital 4, 24.
[84] *Ibid*, article 4.
[85] *Ibid*, recital 22.
[86] EU, *Council Regulation 2021/2085 of 19 November 2021 establishing the Joint Undertakings under Horizon Europe and repealing Regulations (EC) No 219/2007, (EU) No 557/2014, (EU) No 558/2014, (EU) No 559/2014, (EU) No 560/2014, (EU) No 561/2014 and (EU) No 642/2014 2021*, [2021] OJ, L 427, articles 1 and 2.1.
[87] EU Chips Act, article 3 (2).
[88] *Ibid*, recital 31-32.
[89] *Ibid*.

avoid alterations to the internal market[90]. This is an apparent move towards self-preservation of the EU semiconductor industry in a context dramatically dominated by foreign companies.

The final tool supporting industrial transformation for semiconductors is the so-called coordination and mapping mechanism. It represents an effort to strategically track vulnerabilities in order to tackle potential alterations and disruptions to the supply chain[91]. Indeed, the dependency on third countries and potential semiconductor shortages are expressed concerns of the regulation[92]. This coordination and mapping mechanism is coupled with a specific emergency procedure in case of serious disruption to the semiconductor supply chain, which paves the way to a last resort toolbox[93]. Of interest is the possibility in the context of this mechanism to impose "protective measures" on the regional semiconductor industry[94]. It is an open manifestation of the EU willingness to safeguard a key sector for the development of the AI field in conjunction with other essential technologies.

3. Supercomputers and AI Factories

The European High-Performance Computing Joint Undertaking (EuroHPC) gathers the EU, Member States and private participants with the aim to create a supercomputing industry for Europe[95]. Established in July 2021, this project aims at exploiting the use of computing capabilities in different scientific applications. Supercomputers were tasked with a key role in the EU AI strategy, in particular in the context of the recently established AI factories. Indeed, the EuroHPC will also focus on acquiring, developing and improving supercomputers to develop machine learning and training of General-Purpose AI models (GPAI), which consist of AI systems characterised by significant flexibility that can be deployed for a variety of purposes[96].

[90] *Ibid*, recital 57.
[91] *Ibid*, recital 47.
[92] *Ibid*, recitals 47, 57.
[93] *Ibid*, article 23.
[94] *Ibid*, article 24.
[95] EU, *Council Regulation 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488*, [2021] OJ, L 256.
[96] See AI Act, article 3 (63); UE, European Commission, « Commission launches AI innovation package » *European Commission Press Corner*, online: <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383> [Accessed 20 January 2025].

AI factories represent technical ecosystems that allow start-ups to access European public supercomputers and talented human workforce[97]. By the end of 2024, the EU had successfully selected its first seven AI factories[98]. This is an important shift in the EU: originally, computational power of this kind was only available to researchers, while, since 2024, it has become available for European SMEs. This move could also be seen as a form of financial investment by the EU into its regional private sector.

IV. The price of sovereignty: Economic consequences of the EU AI Strategy

The adoption of EU sovereignty-driven policies and regulations in the AI field comes with a cost. Both centrifugal and centripetal approaches of the AI strategy determine a series of economic consequences, which are particularly detrimental vis-à-vis third countries. The existing scholarship so far has not systematically mapped these effects, limiting to analyse the level of influence that the AI Act may have in foreign jurisdictions[99] as well as the environmental concerns derived by the European approach to AI[100]. The following sections aim to start filling this research gap. We will start with an analysis of the economic effects of the EU centrifugal approach to AI sovereignty, which are ensued by the adoption of the AI Act on top of other pre-existing pieces of EU digital law, and will then examine the consequences of the centripetal approach that is attempting to reshore and protect EU AI infrastructures.

A. No land for the weak: The cost of compliance with EU law

[97] UE, European Commission, *Communication on Boosting Startups and Innovation in Trustworthy Artificial Intelligence*, COM (2024) 28 final, 4, at 7.

[98] EUROPEAN HIGH-PERFORMANCE COMPUTING JOINT UNDERTAKING, «Selection of the First Seven AI Factories to Drive Europe's Leadership in AI - EuroHPC JU» *EuropeanHPC Joint Undertaking Press Corner* (10 December 2024), online: <https://eurohpc-ju.europa.eu/selection-first-seven-ai-factories-drive-europes-leadership-ai-2024-12-10_en> [Accessed 20 January 2025].

[99] M. ALMADA AND A. RADU, «The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy» (2024) 25 :, *German Law Journal*, at *646* ; see also C. SIEGMANN AND M. ANDERLJUNG, « The Brussels Effect and Artificial Intelligence », *Centre for the Governance of AI 2022*, online : <https://www.governance.ai/research-paper/brussels-effect-ai> [Accessed 6 March 2025].

[100] See A. PEREZ VICTORIO, E. CELESTE AND A. QUINTAVALLA, «Greening AI? The New Principle of Sustainable Digital Products and Services in the EU» (2024) 61 : *Common Market Law Review*, at 1019 ; S. FALK, A. VAN WYNSBERGHE AND L. BIBER-FREUDENBERGER, «The Attribution Problem of a Seemingly Intangible Industry» (2024) 16 :, *Environmental Challenges*, at 101003 ; see also K. EBERT AND OTHERS, « AI, Climate, and Regulation: From Data Centers to the AI Act », *arXiv,* (2024), online : <http://arxiv.org/abs/2410.06681> [Accessed 6 March 2025]; J. R. LARANJEIRA DE PEREIRA, « The EU AI Act and Environmental Protection: The Case for a Missed Opportunity », *Heinrich-Böll-Stiftung European Union*, online : <https://eu.boell.org/en/2024/04/08/eu-ai-act-missed-opportunity> [Accessed 6 March 2025].

The extraterritorial application of the EU digital regulations is one of the core strategies of what we have earlier defined as the centrifugal approach to EU regulation pursuing digital sovereignty objectives. From an economic perspective, it represents a main concern for non-EU businesses. We cannot deny that both local and foreign companies must undertake an adaptation of their processes or design new ones in order to meet the standards set by EU law. Nonetheless, it is apparent that third party countries' financial onus is higher. This can be explained due to the fact that EU regulatory standards are usually stricter than foreign ones. This allows EU companies implementing local rules to operate outside of the EU with reduced compliance cost, while the other way around does not hold true. Non-EU businesses have to ensure compliance with the more severe EU standards as well as very often pay the cost to establish a legal representative in the EU, as various pieces of EU law require.

Even though the AI Act will enter into full force in August 2026, businesses must start making necessary arrangement to comply with it[101]. Failure to do so exposes companies to potential harsh penalties. These adaption costs add up to the ones imposed by other regulations like the GDPR and of course, the DA and DGA. Non-EU companies are placed in a financial vulnerable position. Unlike local EU businesses (either big corporations or SMEs), foreign companies developing AI systems abroad cannot be beneficiaries of EU financial support measures. As we have seen, a common aspect of the EU AI strategy is the prioritisation of European capacities. This feature could turn a common operational expenditure into a structural disadvantage for foreign competitors.

The estimation of compliance cost for businesses, either providers or deployers of AI technologies, raises up to € 333,000[102]. Yet, not all businesses will live up to the investment required. The size of the company would heavily influence whether it could bear the costs of satisfying EU legal standards or if it makes operations in the EU unfeasible. It is likely that overseas tech giants will be the only "survivors" of this conformity to the AI Act as they are less vulnerable and their large market share is a guarantee of profitability[103]. This could pave the way to foreign monopolies of big corporations while hampering innovation from foreign SMEs.

---

[101] AI Act, recital 179.

[102] A. ADIMI GIKAY, «Risks, Innovation, and Adaptability in the UK's Incrementalism versus the European Union's Comprehensive Artificial Intelligence Regulation» (2024) 32 *International Journal of Law and Information Technology*, at 13.

[103] W. WU AND S. LIU, «Compliance Costs of AI Technology Commercialization: A Field Deployment Perspective» *arXiv*, (2023), online: <http://arxiv.org/abs/2301.13454> [Accessed 20 January 2025], at 1.

Higher costs due to unilateral stricter EU regulation is an old foe. The GDPR produced a drastic increase in compliance expenses by foreign businesses[104]. It took a toll on the revenue, profitability and market access for companies operating in Europe[105]. There were instances in which companies claimed their budget to be insufficient to cover the expenses for GDPR-derived obligations[106]. Said arguments are interesting because they affect the behaviours of companies outside of the EU. Some non-EU businesses pursued a cautious approach to the European market, reducing their exposition to its legal system[107], while other companies decided to relocate themselves or even refrained to offer their services in the EU as preventive measures[108].

As the regulatory landscape of the EU evolves and raises its complexity, it could be argued that the legal battle to preserve European values by adopting strict regulatory standards indirectly deters foreign competitors — or at least the financially modest ones — from accessing the EU single market. It remains to be seen how levelled the playing field will be once all the regulatory components of the EU digital strategy will be fully in force.

B. Going local: Subsidies, tariffs and additional measures

The EU unwavering support to local AI and related technologies industries is manifest in the policies and legislation discussed in the previous section. This has translated into providing substantial public funding, facilitating administrative procedures and fostering the resilience of the supply chain.

Financial assistance to EU business has been mainly granted at two levels: first, through EU existing programmes that target innovation and digital transition, and second, resorting to contributions provided at national level by Member States. The latter underscores substantial changes in EU policymaking. State aid and its legality is regulated by Articles 107 to 109 of

---

[104] C. PEUKERT AND OTHERS, «Regulatory Export and Spillovers: How GDPR Affects Global Markets for Data», *CEPR* (30 September 2020), online: <https://cepr.org/voxeu/columns/regulatory-export-and-spillovers-how-gdpr-affects-global-markets-data> [Accessed 20 January 2025].
[105] G. JOHNSON, «Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond », online: <https://www.nber.org/system/files/working_papers/w30705/w30705.pdf> [Accessed 18 January 2025], at 19.
[106] World Bank Group, A. CHANDER AND OTHERS, *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation*, Policy Research Working Paper, N°9594, online: <https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3392&context=facpub> [Accessed 20 January 2025], at 12.
[107] *Ibid*.
[108] M. N. LINTVEDT, «Putting a Price on Data Protection Infringement» (2022) 12 *International Data Privacy Law*, at 1.

the Treaty on the Functioning of the European Union (TFEU). Generally, financial support given by Member states to industries is not compatible with the EU Single Market due to the distorting effects for trade and competition within the bloc, with some exceptions laid out in the aforementioned provisions.

Already in 2022, the European Commission adopted a revised framework to loosen state aid regulation for the purpose of research and development and innovation[109]. This change was introduced to provide tactical support to the green and digital transition[110]. The perimeter of the exceptions includes a variety of "digital industries" such as artificial intelligence, cloud, edge technologies and supercomputing, among others[111]. In plain terms, aware of the imperative need to boost the local industrial sector, the EU is allowing subsidies from Member States. This is accompanied by frequent references in the EU Chips Act to public support and incentives[112]. Despite there is no clarification yet about the extent or nature of these incentives, the EU is setting the legal foundations to allow direct participation - or intervention - from its Member States to contribute to the development of local industrial capacity. Similarly, the fast-tracking of permit granting procedures regarding the planning, construction and operation of integrated production facilities and open EU foundries established in the aforementioned regulation, places EU businesses in a preferential position.

Finally, the broad reference to "protective measures" issued in the context of Article 14 of the EU Chips Act raises the question on the materialization of tariffs or similar duties. Whereas the regulation is not clear about it, the growing tendency of the EU to support and defend its industrial development may lead, for instance, to the imposition of tariffs on imports in digital technologies ranging from end products to components. By establishing supportive measures in compliance with EU law to fulfil its objectives, the bloc could adopt practices with a significantly adverse effect on foreign competitors.

V. Assessing protectionist trends in the EU AI Strategy

[109] UE, European Commission, *Communication from the Commission Framework for State aid for research and development and innovation*, 2022/C 414/01 2022.
[110] UE, European Commission, «State aid: Commission adopts revised State aid Framework for research, development and innovation», *European Commission Press Corner*, (19 October 2022), online: <https://ec.europa.eu/commission/presscorner/detail/ en/ip_22_6233> [Accessed 22 January 2025].
[111] *Ibid.,* at 8.
[112] See section III.B.ii above.

A. The rise of digital protectionism

Traditionally, the concept of protectionism referred to actions "altering market conditions and distorting trade in ways that favour domestic producers over their foreign competitors"[113]. In the digital field, what has been called 'digital protectionism' is a materialisation of a stringent domestic conception of the digital economy according to which nations try to limit digital activities with an economic impact within national borders and to exert control over cross-border digital operations[114]. Aaronson suggests that it entails the "erection of barriers or impediments to digital trade", mentioning also regulatory techniques that go beyond those traditionally used in the economic field, such as "censorship, filtering, localization and regulations to protect privacy", which might not primarily aim to create economic effects, but *de facto* create barriers to economic players[115].

Overall, digital protectionism could be described as a form of shielding of the digital national industry and economy to reduce vulnerabilities vis-à-vis foreign competitors, tackling dependencies and safeguarding national security. Digital protectionism might be considered as a byproduct of digital *sovereigntism*, intended as an abusive manifestation of digital sovereignty[116]. From an economic point of view, protectionism generates income losses, stifles investment and, overall, slows down economic growth[117]. Naturally, trade barriers impact global trade, generating a knock-on effect on the supply chain and on all the businesses dependent on it[118]. Protectionism leads to fragmentation and isolation. By establishing protectionist measures, countries erode the world trade system, favouring local competitors and only selected foreign allies, reinforcing geopolitical divisions, through national 're-shoring' or 'friend-shoring' dynamics[119]. Non-discrimination is deemed a core tenet of international trade law that promotes an equal treatment between foreign and local economic operators[120]. As

---

[113] S. AARONSON, « What Are We Talking about When We Talk about Digital Protectionism? » (2019) 18 *World Trade Review 541*, at 3.
[114] Georgia Tech, «Digital Free Trade» *Internet Governance Project*, online: <https://www.internetgovernance.org/project/digital-free-trade/> [Accessed 7 August 2024].
[115] S. AARONSON, «What Are We Talking about When We Talk about Digital Protectionism?», *op. cit,* at 8.
[116] See E. CELESTe, «Brexit and the Risks of Digital Sovereignism», *op cit.*; see also E. CELESTE «Digital Sovereignty in the EU: Challenges and Future Perspectives», *op. cit.*
[117] A. PIEKUTOWSKA AND P. KONOPKA, «How to Measure Protectionism in International Trade in XXI Century? The Regional Barometer of Protectionism – Case of Poland» (2023) 29 *Technological and Economic Development of Economy*, 775, at 776.
[118] *Ibid*.
[119] M. DABROWSKI, «The Risk of Protectionism: What Can Be Lost?» (2024) 17 *Journal of Risk and Financial Management*, at 374.
[120] W. DAVEY, *Non-Discrimination in the World Trade Organization: The Rules and Exceptions*, vol 14, Brill, 2012, at 55; see also N. DIEBOLD, «Standards of Non-Discrimination in International Economic Law» (2011) 60, *International & Comparative Law Quarterly*, at 831.

global trade rules are disregarded, by putting in place barriers to foreign economic operators, a de-globalization trend emerges, fragmenting the trade legal framework and progressively isolating countries.

Digital protectionism has usually been associated with the imposition of barriers to digital trade and cross-border flows of data with a focus on data localisation requirements[121]. In this chapter, we propose a broader interpretation of this concept. Beside the aforementioned aspects, it could incorporate expressions of protectionism which affect any aspect of the digital supply chain, thus not limited to barriers to international data flows. Broadening the scope of the term would allow to better highlight the link between digital sovereignty strategies and current trade policies and instruments. For instance, the abovementioned distorting measures surrounding semiconductor components adopted in the US could amount to this enlarged view of digital protectionism, which pursues primacy in the technological domain. The same could apply to our current discussion on the EU approach to digital law and policy, particularly for the development of AI.

Over the past few years, the phenomenon of protectionism has been steadily resurfacing around the globe. Already by 2017, more than 50% of exports from G20 members — among which we can find the EU — had been subjected to harmful trade measures[122]. Similarly, on a global scale, between 2021 and 2024, a considerable number of harmful policy instruments affected trade of goods and services[123]. Likewise, the EU has incorporated in its regulatory repertoire instruments for the preservation of its economy. For instance, the Foreign Direct Investment Regulation, and the Anti-Coercion Regulation, which address aspects such as screening of foreign direct investment and economic coercion by third countries, respectively. Recently, the EU prolonged steel safeguard measures until June 2026 in an effort to keep protecting EU steel producers[124]. Likewise, the European Commission imposed countervailing duties on imports of electric vehicles' batteries coming from China, as they were beneficiaries of unfair

[121] S. AARONSON, « What Are We Talking about When We Talk about Digital Protectionism?», *op cit.* see also Poland, The Polish Institute of International Affairs 2021, O. SZYDŁOWSKI, *Digital Protectionism: Data Locatisation*, N°22 (208), online: <https://pism.pl/publications/digital-protectionism-data-localisation> [Accessed 6 March 2025]; see also F. LANCIERI, «Digital Protectionism? Antitrust, Data Protection, and the EU/US Transatlantic Rift» (2019) 7 *Journal of Antitrust Enforcement*, at 27.

[122] EU, European Central Bank, *The Economic Implications of Rising Protectionism: A Euro Area and Global Perspective*, 24 April 2019, online: <https://www.ecb.europa.eu/press/economic-bulletin/articles/2019/html/ecb.ebart201903_01~e589a502e5.en.html> Accessed 20 January 2025.

[123] «Global Trade Alert - Monitoring Policy Changes That Affect Global Trade», online: <https://globaltradealert.org/> [Accessed 20 January 2025].

[124] UE, European Commission, «EU Prolongs Steel Safeguard Measure until June 2026», 25 June 2024, online: <https://policy.trade.ec.europa.eu/news/eu-prolongs-steel-safeguard-measure-until-june-2026-2024-06-25_en> [Accessed 20 January 2025].

subsidies that were causing economic damage to EU battery electric vehicles manufacturers[125]. Even though these may not strictly speaking classify as a protectionist expression, this trend reveals that the EU is also ready to implement trade defences to protect the local industry. In fact, this position has been recently confirmed by EU Commission's President Von der Leyen, who expressed that the EU will preserve its interests "however and whenever needed" in response to current global trade frictions[126], which have intensified since January 2025.

B. Between protectionism and open strategic autonomy

Against this backdrop, it is worth questioning to what extent EU AI policies adopt measures that could be considered as expressions of digital protectionism. From a theoretical perspective, all the components of the EU regulatory digital package, meaning the AI Act, Data Act, Data Governance Act, and mostly the Chips Act, erect and consolidate trade barriers[127]. They create legal requirements that are akin to those that Aaronson mentioned as triggers of digital protectionism. The AI Act, for example, has been criticised for imposing obligations on non-EU companies due to its extraterritorial effect[128], and accused of protectionism for not involving third countries' standardisation bodies[129]. While the rationale of these laws is the creation of an AI industry made in the EU, their requirements represent a serious disadvantage to overseas competitors due to the cost of implementation and adaptation. Likewise, the concerns of protectionism are stronger if we consider current public funding available to EU companies and the relaxation of state aid rules discussed above. This whole panorama has a rather distortive impact to competition and international trade[130]. Protectionism seems to make its way into EU digital law.

---

[125] I. GARCÍA BERCERO, «EU Duties on Chinese Electric Cars Are a Rule-Respecting Response to Subsidies», *Bruegel* (27 November 2024), online: <https://www.bruegel.org/first-glance/eu-duties-chinese-electric-cars-are-rule-respecting-response-subsidies> [Accessed 20 January 2025].

[126] UE, European Comission, *Speech by the President: EU Ambassadors Conference 2025*, *European Commission*, 4 February 2025, online : <https://ec.europa.eu/commission/presscorner/detail/pl/speech_25_404> [Accessed 7 February 2025], at 2.

[127] See A. CALDERARO AND S. BLUMFELDE, «Artificial Intelligence and EU Security: The False Promise of Digital Sovereignty» (2022) 31 *European security*, at 415.

[128] H. SCHNEIDER, « Europe's AI Regulation Will Stifle Innovation », *GIS Reports*, 10 October 2024, online: <https://www.gisreportsonline.com/r/ai-act-eu-regulation-innovation/> [Accessed 25 February 2025].

[129] N. CORY AND P. GRADY, «The EU's Approach to AI Standards Is Protectionist and Will Undermine Its AI Ambitions», *Center for Data Innovation* (6 February 2023), online: <https://datainnovation.org/2023/02/the-eus-approach-to-ai-standards-is-protectionist-and-will-undermine-its-ai-ambitions/> [Accessed 20 January 2025].

[130] M. BAUER AND D. PANDYA, «EU Autonomy, the Brussels Effect, and the Rise of Global Economic Protectionism», *European Centre for International Political Economy Occasional Papers* (February 2024), online: <https://ecipe.org/publications/eu-autonomy-brussels-effect-rise-global-economic-protectionism/> [Accessed 20 January 2025], at 5.

However, despite the ineluctability of such a theoretical reconstruction, if we take a practical and more comprehensive perspective, our initial conclusion has to be qualified. First of all, the majority of these regulatory measures has been recently implemented. This limits the availability of data to measure and accurately determine concrete effects of the EU AI Strategy on global trade and whether third countries have effectively suffered losses since the entry into force of the above-mentioned tools.

Secondly, potential protectionist attitudes adopted by EU regulation should be more broadly contextualised. At the moment, for example, one of the mantras of the EU policy agenda is represented by the objective of fostering competitiveness. Protectionism alone does not achieve this objective if not paired with targeted international cooperations with selected third countries. Consequently, a strategic partnership approach with third countries has been suggested, for instance, to diversify the raw materials supply chains, which impacts equally the semiconductor value chain and green technologies[131].

Protectionist trends here become part of a more comprehensive image that sees the EU aiming to defend its strategic autonomy in an open way, without resorting to full closure, but by fostering collaboration with like-minded countries. Not only is the EU trying to reshore its critical industries within the Union, but the scholarship has also rightly spoken of phenomenon of "friend-shoring"[132]. Current EU strategies like the Global Gateway and Team Europe are clear examples of such an "open" approach of the Union. The Global Gateway was introduced in 2021 with the goal of investing up to 300 billion Euros in infrastructure development between 2021 and 2027[133]. This flagship programme aims to connect the EU with third countries by helping them to boost economic and societal development while fostering opportunities for the Union's private sector[134]. The Global Gateway is a value-based, transparent and sustainability-oriented investment policy to keep the EU connected with the rest of the world. This project is delivered via 'Team Europe' that can be seen as an operational investment collective. Team Europe brings together different levels of resources and expertise, such as the EU, Member States, the European Investment Bank and the European Bank for

[131] M. DRAGHI, «The future of European competitiveness Part B: In-depth analysis and recommendations», at 57, 61, 90, 136, 157.
[132] O. FONTANA AND S. VANNUCCINI, «How to Institutionalise European Industrial Policy (for Strategic Autonomy and the Green Transition)», (2024) 24 *Journal of Industry, Competition and Trade*, at 1.
[133] UE, European Commission, *The Global Gateway*, Joint Communication, JOIN (2021) 30 final.
[134] *Ibid*.

Reconstruction and Development[135]. Originally set in place to address the challenges of the COVID-19 pandemic[136], it became the main mechanism to deploy and implement the objectives of the Global Gateway. Although more selective, the EU continues to forge stable connections around the world.

Thirdly, there are mounting critiques to the EU proactive approach to digital regulation, which, especially in the AI field, is accused to stifle innovation[137]. EU protectionism in this field might have to be rethought to guarantee the access by individuals, businesses and researchers to the latest and most advanced AI systems developed in third countries. Lastly, the recent economic and geopolitical scenario has significantly changed after the re-election of Donald Trump. The EU has now to react to aggressive economic policies adopted not only by China, but also by its historical ally and main trade partner, the US. Protectionist attitudes could thus be interpreted as a reaction to these geopolitical external pressures[138], rather than as an EU spontaneous economic policy.

VI. Conclusion

EU AI policies represent a cornerstone of the Union's current strategy towards the digital transformation. In contrast to two decades ago, where the mantra of digitalisation was securely accompanied by economic neo-liberalism, today we witness the consolidation of digital sovereignty as a guiding principle of the EU digital strategy. Digital sovereignty emerges as a 'silent' driver, yet with very concrete economic effects. We do not have a single policy instrument articulating explicitly how this notion should drive AI policies. However, the direction that AI policies take in the EU, when guided by digital sovereignty ambitions, strengthens the idea that the EU is increasingly protectionist, progressively disfavouring non-EU players to consolidate an AI industry made in the EU.

---

[135] UE, European Commission, «Team Europe Initiatives » *European Commission - International Partnerships* (20 February 2025), online: <https://international-partnerships.ec.europa.eu/policies/team-europe-initiatives_en> [Accessed 6 March 2025].

[136] UE, European Commission, *The Global EU response to COVID-19*, Joint Communication, JOIN (2020) 11 final.

[137] M. DRAGHI, «The Future of European Competitiveness Part A», *op. cit.*, at 14, 26; see also J. S. MARCUS AND M. ROSSI, «Strengthening EU digital competitiveness: Stocking the engine» (2024), *European University Institute*, 11.

[138] M. SHEN AND M. YANG, «Are Geopolitical Risks Fuelling Trade Protectionism?», (2024) 35, *Defence and Peace Economics*, 1120, at 19.

In this chapter, we contributed to the existing scholarship in two ways: firstly, by reconstructing how the EU is pursuing an AI strategy in a digital sovereignty-oriented manner, and, secondly, by examining the economic effects of this trend. Digital sovereignty supports the creation of EU AI standards with a potential global effect: the AI Act is expression of what we called a 'centrifugal' expression of digital sovereignty ambitions. This tendency of exploiting the EU normative power on a global scale is not new; it leverages the EU's uniqueness in terms of international trade weight and influence, but today it is crucial to complement what we called the 'centripetal' way of articulating AI policies in a digital sovereignty-oriented manner. The EU is indeed trying to reshore key components of the AI industry on European soil through a set of centripetal policies. Many of these regulatory interventions are underpinned by significant financial aids.

This scenario of a progressively closing EU AI industry supported by stringent standards is what led to the analysis of the economic effects of this trend in the second part of this chapter. The AI Act, as the GDPR before, is creating higher costs of compliance for non-EU players (and not only). The EU intervention in the protection of the newborn EU AI industry unavoidably shields local players. Is this sufficient to speak of an emerging digital protectionism in the EU AI field? In the last part of our chapter, we clarified that theoretically this is possible, if we expand the current conception of 'digital protectionism' as to encompass economic consequences favouring local players that are not necessarily related to the adoption of localisation requirements, but result from the introduction of any type of digital policies. Yet, we clarified that this conclusion has to be qualified by the current economic and geopolitical scenario that the EU is facing. Rather than a strict protectionism, the EU seems to be prone to foster strategic partnerships. The Union alone cannot be sovereign in the AI sector in the short to medium term. There are key components of the AI life cycle that cannot be sourced in Europe. The US and China are advancing rapidly. In order to foster its competitiveness, the EU embraces an autonomy strategy that is no longer as open as in the past, but cannot certainly consist of blind protectionism. The question for the EU AI future seems to lie in the extent of its strategic openness.