PromethEUs

PROMETHEUS PUBLICATION

A BLUEPRINT FOR THE DIGITAL PRIORITIES OF THE NEW EU MANDATE

EXECUTIVE SUMMARY

Chapter 1: From Complexity to Clarity: Improving EU digital regulation for a competitive Single Market

The European Commission of 2019-24 undertook a large number of initiatives to create a legal and regulatory framework for a digital environment that is secure, fair and inclusive, and nurtures competitive and innovative markets while protecting EU citizens' values and fundamental rights. In this context, however, **digital providers face the challenge of navigating over 100 existing and forthcoming laws**, a complex landscape that proves demanding even for large firms. These regulations, including the Digital Markets Act, Digital Services Act, and other key frameworks like the Data Governance Act and AI Act, aim to harmonise practices, ensure user safety, and support the EU's digital transformation goals.

As the EU enters the second half of the Digital Decade, it aims to balance innovation, competition, and protection of citizens through its regulatory framework, such as the AI Act to reduce AI-related risks, and finalising guidelines such as the AI Pact to promote transparency and accountability. Simultaneously, frameworks like the NIS2 Directive and the proposed ePrivacy Regulation underscore the EU's commitment to enhancing cybersecurity and safeguarding confidentiality of communications. However, reports such as those of Letta and Draghi emphasise the need for streamlined regulations, reduced barriers for SMEs, and harmonised frameworks to foster growth, innovation, and competitiveness across sectors.

The new European Commission has indeed set an ambitious agenda to drive digitalisation, innovation and regulatory efficiency, emphasising fostering competitiveness while maintaining sustainability and fairness. **Henna Maria Virkkunen**, Executive Vice-President for Tech Sovereignty, Security and Democracy, highlighted the EU's twin strategy of boosting investment in frontier technologies such as AI, quantum computing and cloud services, and ensuring a secure level playing field for companies operating under European rules. Complementing this, **Valdis Dombrovskis**, Commissioner for Implementation and Simplification, emphasised **cutting red tape, streamlining regulations, and promoting digital tools such as data spaces and digital wallets** to reduce administrative burdens, especially for SMEs.

Chapter 2: Strategic Investment for a Competitive Digital Future

The **European Union** has a unique opportunity to establish itself as a major player in the global technology landscape. However, nowadays, **the EU depends on third countries for more than 80% of its digital products, services, infrastructure and intellectual property (IP)**, unlike the US and China which have shifted their economic model towards ICT.

The lack of a technological strategy and **lower public and private investments** weigh on the **EU's competitive position** and the risk is for Europe to become totally dependent on technologies designed and developed abroad.

For example, in the **AI technology field**, the European Union still has a long way to go. While the development of EU AI plans is broadly in line with international best practices, the investment is still too low compared to US and China.

Looking at the data, the US is leading in AI **private investment** ($ 67.2 bn) in 2023, followed by China ($ 7.8 bn). The amount of investments in AI by the US was roughly 8.7 times greater than that invested in China and 17.8 times of that invested in the United Kingdom ($ 3.8 bn). The top three EU countries in the ranking (Germany, Sweden and France) reported a total value of AI private investment (about $5.50 bn) slightly higher than that recorded by the United Kingdom alone. **The AI investment gap between the US and the EU has been widening over time**. In fact, while AI private investments have decreased in the EU plus the UK (-14.1%) since 2022, the US has seen a significant increase (22.1%) during the same period

OECD data has also highlighted the gap between the EU, the US and China in the amount of VC investment in AI. However, the EU recorded a positive trend in venture capital investment with an appreciable increase of 91% in the period 2019-2023.

Moreover, **Europe suffers from very limited private investments in quantum technologies compared to other countries**. According to Mario Draghi's report, EU firms attract only 5% of global private funding compared with the 50% attracted by US firms. China and the United States, moreover, hold technological leadership in most critical components or materials for quantum computing platforms.

The Digital Europe Programme strengthens investment in a range of areas including semiconductors. However, despite the Chips Act, overall investment and public support for semiconductor production in the EU remains below that in the US.

In light of these considerations, **the current budget of the Digital Europe Programme (less than € 10 bn over 7 years) is not sufficient to bridge the gap between the EU and the US and China.**

Therefore, aspects such as the regulatory framework or financial support need to be thoroughly rethought to ensure that the **EU can grow independently and truly competitively**.

Chapter 3: Empowering SMEs: The Role of Upskilling, Reskilling, and Sectoral Dataspaces in Southern Europe

Small and Medium-sized Enterprises are central to the economies of Southern Europe, representing a significant proportion of employment and GDP in Spain, Portugal, Italy, and Greece. These enterprises **are navigating profound challenges as the region transitions toward digitalization and sustainability**, which are key pillars of the European Union's strategic vision. Specific initiatives are designed to address the skill gaps and technological integration needs of SMEs to harness the transformative potential of upskilling and reskilling programs and of sectoral dataspaces. **Upskilling programs are critical in equipping SME workforces with digital and green capabilities**, ensuring their **competitiveness, sustainability, and resilience against market shifts**. Sectoral dataspaces complement these efforts by fostering secure and collaborative data-sharing ecosystems within key industries such as agriculture, energy, healthcare, and mobility, enabling innovation and cross-border cooperation.

Despite their potential, SMEs face significant obstacles, including **inadequate digital infrastructure in rural areas, financial and administrative barriers, and cultural resistance to adopting new technologies.** National governments and EU institutions expend efforts to mitigate these challenges through funding mechanisms like COSME and the European Social Fund, alongside tailored programs such as Reskilling for Employment and DIS4SME. Additionally, **sectoral dataspaces**, such as the European Mobility Data Space and the European Health Data Space, **are transforming industries by leveraging data-driven solutions to enhance efficiency and sustainability**.

Through targeted interventions and cross-sector collaboration, **Southern Europe is poised to unlock the full potential of SMEs**. By addressing skill gaps, fostering innovation, and creating supportive ecosystems for data sharing, these initiatives aim to build a sustainable and competitive economic landscape. **The aligning of regional efforts with broader EU objectives**, such as the European Green Deal and Digital Decade targets, **is critical to ensure inclusive and resilient growth** across Southern Europe.

Chapter 4: Priorities for the international agenda of EU’s digital policy in the 2024-2029 mandate

If the European Union’s perspective has been since 2019 focused on sovereignty and open strategic autonomy, **the new mandate in 2024 kicks off with a paradigm shift towards economic security**. Also, a second layer of this transformation is marked by the transition from a regulatory focus into a **new approach oriented to industrial policy, public intervention and competitiveness** as the vertebral axis of digital and clean transitions and a stronger defense baseline.

These transformations over the 2019-2024 period have contained an international angle. This chapter addresses four main policy angles that the new mandate for the 2024-2029 period should include in the international dimension of EU’s digital policy:

(a) The institutional and governance dimension with the creation of first-ever Executive Vice-President for Technology Sovereignty, Security and Democracy;

(b) The strengthening and further coordination of digital diplomacy efforts;

(c) The technological dimension in the Enlargement Policy mostly with candidate countries to access the European Union;

(d) Revamped agenda with priority-setting and an action-based roadmap for putting the Economic Security Strategy into practice.

CONTRIBUTORS

Chapter 1: From Complexity to Clarity: Improving EU digital regulation for a competitive Single Market

IPP-Lisbon & I-Com, Institute for Competitiveness
Steffen Hoernig, Alessio Caramitti, Alessandro D'Amato

Chapter 2: Strategic Investment for a Competitive Digital Future

I-Com, Institute for Competitiveness
Stefano da Empoli, Maria Rosaria Della Porta

Chapter 3: Empowering SMEs: The Role of Upskilling, Reskilling, and Sectoral Dataspaces in Southern Europe

The Foundation for Economic & Industrial Research (IOBE)
Valaskas Konstantinos, Aggelos Tsakanikas

Chapter 4: Priorities for the international agenda of EU's digital policy in the 2024-2029 mandate

Elcano Royal Institute
Raquel Jorge Ricart

Table of Contents

Chapter 1: From Complexity to Clarity: Improving EU digital regulation for a competitive Single Market

1.1 A diagnosis of the current digital regulatory framework

The **European Union's *Digital Decade Policy programme* of 2022** was formulated as a strategic vision for Europe's digital transformation by 2030, aiming to boost digital skills, infrastructure, and technology across the EU[i]. In a complementary development, the European Commission of 2019-24 undertook a large number of initiatives to create a legal and regulatory framework for a digital environment that is secure, fair and inclusive, and nurtures competitive and innovative markets while protecting EU citizens' values and fundamental rights. Regarding this, Zenner, Marcus and Sekut (2024) compiled an **overview of EU laws that affect the digital economy**[ii]. **As of June 2024**, they counted **87 applicable laws, 21 laws in the legislative process, and 8 planned initiatives**. Evidently, complying with so many laws and regulations, even if not all do apply to the same companies, is hard even for larger firms.

Furthermore, the **proliferation of digital regulations** and the **gradual shift of key policy decisions in this area to European institutions** – along with the increasingly central role assumed by the European Commission (evidenced by the powers conferred upon it by the Digital Markets Act) – is prompting a reconsideration of the already delicate balance between regulation and competition protection. It thus appears pertinent to provide an overview of the principal **EU-derived legal acts**, whether in the form of regulations or directives, that are **currently in force**. This will help understand how they interconnect and where they overlap, with significant implications for the implementation phase of these various norms and, consequently, for the operational activities within and across organisations.

In 2022, Regulation 2022/1925 on fair and contestable markets in the digital sector, otherwise known as the **Digital Markets Act (DMA)**, was adopted. This regulation, which employs an *ex-ante* approach, seeks to proactively prevent the exploitation of dominant positions before they result in competitive harms. The ultimate objective is to reduce the dominance of large digital platforms and to foster a more open, innovative and competitive digital environment for European businesses and consumers. The **DMA provides the European Commission with a set of powers** similar to those typically exercised by antitrust authorities. These include the ability to conduct inspections, issue information requests, question company employees, impose interim measures, undertake market investigations and, most significantly, impose sanctions. Also, the **DMA does not undermine the application of national competition rules,** by establishing a robust set of obligations and prohibitions for gatekeepers (e.g., sharing data with smaller competitors, preventing discriminatory practices against third parties, and ensuring data portability for users). It should be noted that the national rules, including those that prohibit other forms of unilateral conduct, remain applicable insofar as they target entities other than gatekeepers or impose additional obligations on gatekeepers.

In the same year, Regulation 2022/2065 on a Single Market for Digital Services was adopted as a complement to the DMA. More in detail, the **Digital Services Act (DSA)** introduces comprehensive provisions for digital services with the objective of ensuring a safer online environment for users. In a similar manner to the DMA, the DSA enhances the regulatory powers of the European Commission. It is noteworthy that this Regulation imposes an obligation on hosting service providers to act expeditiously by **removing or disabling access to illegal content** as soon as they become aware of it. Furthermore, it establishes liability exemptions for digital intermediaries for online content, confirming the absence of any general obligation to monitor or actively investigate content. In lieu of imposing direct obligations, this framework imposes due diligence obligations and sets out rules for enforcement, cooperation, penalties, and implementation to address the various risks identified within the legislation, including the dissemination of illegal content online.

Considering the growing importance of the data economy, the EU has taken the initiative to draw up a comprehensive Data Strategy. The **EU Data Strategy**, presented in 2020, involves a five-year plan, presents a vision of a data-driven economy in the EU, and sets out guidelines for the future regulatory framework. The aim is to guarantee the free flow of data within the EU and across sectors, optimising its potential for innovation. Furthermore, the Data Strategy proposes the establishment of **unified European data spaces** to facilitate the sharing and pooling of data across the EU and across sectors. The Data Governance Act (DGA) and the Data Act (DA) are two pivotal stages in the implementation of the European Data Strategy.

Regulation 2022/868, known as the **Data Governance Act (DGA)**, was enacted in 2022 to establish the conditions for the **re-use within the Union of certain categories of data held by public entities**. This includes data protected for reasons of commercial confidentiality, statistical confidentiality, third-party intellectual property rights, and personal data protection, provided that it does not fall within the scope of Directive 1024/2019. In particular, the DGA establishes a framework for the reuse of protected data held by public entities and prohibits public bodies in Member States from entering into exclusive data-sharing agreements or granting exclusive rights to any entity. Furthermore, the DGA introduces the concepts of "**Data Intermediation Service Providers**" (DISPs) and "**Data Altruism Organisations**" (DAOs), as well as defining the rules that govern the transfer of data to third countries.

Regulation 2023/2854 on harmonised rules for fair access to and use of data (**Data Act - DA**) came into force on 11 January 2024 and will be applicable as of September 2025. It elucidates the circumstances under which entities may derive value from data, pursuing the aim of establishing a fairer, more efficient, and **interoperable data ecosystem**. This will be achieved by fostering innovation while protecting the interests of users and data holders. More in detail, the **DA addresses**

both personal and non-personal data, establishing harmonised rules for: (a) the availability of data from connected products and related services to users of those products or services; (b) the provision of data by data holders to data recipients; (c) the provision of data by data holders to public bodies, the European Commission, the European Central Bank, or Union bodies in exceptional cases where such data is needed for a specific task carried out in the public interest; (d) the facilitation of switching between data processing services; (e) the introduction of safeguards against unauthorised third-party access to non-personal data; (f) the development of interoperability standards for accessing, transferring, and using data.

In relation to the aforementioned **implementation phase**, DA Recital no. 10 stipulates that this framework is applicable without prejudice to the DSA, whereas DA Recital no. 36 explicitly emphasises its consistency with the DMA. Furthermore, Article 5.2 of the DA excludes any entity classified as a "gatekeeper" under the DMA from being considered a third party for data access rights. Nevertheless, **some ambiguity persists about the relationship between the different legal instruments**. For instance, the DA is applicable to data generated by IoT devices, yet excludes derived or inferred data. Moreover, neither the DA nor the DSA contain provisions preventing gatekeepers from acquiring data-holding rights or purchasing companies that hold data. This is a notable aspect, as the DA seems to impose limitations on gatekeepers regarding acquiring generated data directly from IoT device manufacturers.

Furthermore, the **governance models exhibit considerable divergence**. The DMA adopts a centralised governance structure, with the European Commission playing a leading role. In contrast, the DA relies on a decentralised and potentially fragmented approach at the national level. The DA allows for the designation of various national competent authorities while preserving the jurisdiction of existing bodies, such as those responsible for data protection or electronic communications regulation. In cases where multiple authorities coexist, the DA requires the identification of a coordinating competent authority, which further adds to the complexity of its governance structure.

In a context where data has become an indispensable resource, Member States were required to incorporate Directive 2019/1024 (**Open Data Directive - ODD**) into their national legislation by 17 July 2021. No sooner than 17 July 2025, the European Commission will evaluate the Directive and submit a report on its main findings to the European Parliament, the Council and the European Economic and Social Committee. The ODD is based on the premise that **public sector information represents an invaluable source of data** with the potential to enhance the internal market and facilitate the development of new applications. Furthermore, the strategic application of data, including its processing through artificial intelligence applications, has the potential to transform all sectors of the economy. In order to achieve this objective, **the ODD establishes minimum standards for the reuse of public sector information** and provides practical measures to facilitate the reuse of existing documents held by public sector bodies of Member States, publicly owned companies, and research data.

Following a protracted and intricate legislative procedure, Regulation 2024/1689 (**AI Act**) was formally promulgated in the Official Journal of the European Union on 12 July. The regulation will become **fully applicable by 2 August 2026**, with earlier deadlines for specific cases. The AI Act applies to a **wide range of entities**[1]. From a methodological perspective, the AI Act is structured around differentiated obligations based on a **risk-based approach**. This approach categorises AI systems into three distinct categories - unacceptable risk, high risk and limited risk.

On 8 December 2024, **Directive 2024/2853** came into force with the objective of modernising and harmonising the EU rules **on liability for damage caused by defective products**, considering technological advancements. In accordance with the stipulations set forth in the directive, **its provisions are also applicable to artificial intelligence systems within the scope of the AI Act, subject to the fulfilment of specific conditions**. For instance, Article 10 establishes that non-compliance with mandatory safety requirements under the AI Act gives rise to a presumption of product defectiveness and a causal link to the harm suffered, thereby reducing the burden of proof for the injured party. In comparison to the previous legislative framework (Council Directive 85/374/EEC), this new framework considerably broadens the: (a) **definition of "product"**, which has been expanded to include all movable goods, including software; (b) the scope of liability is expanded to **encompass all economic operators in the production chain**, as opposed to being limited to the manufacturer; (c) the concept of **"damage to data"** is explicitly recognised as a compensable form of harm. **The deadline for Member States to transpose this directive into national law is 9 December 2026**. It will exclusively apply to products placed on the market or put into service after this date.

In an ecosystem that is becoming increasingly oriented towards the digitalisation of resources and services, **the European Union initiated its cybersecurity efforts in 2013 with the introduction of its inaugural strategy in this field**. Subsequently, the EU has pursued a programme of legislative initiatives with the objective of ensuring the optimal security of the digital ecosystem. A pivotal role within this framework is played by the EU Agency for Cybersecurity (ENISA). During the most recent European legislative term, **the cybersecurity regulatory framework has undergone a significant expansion, incorporating numerous new elements**. This has led to a notable increase in the complexity faced by entities subject to a variety of obligations under the evolving regulatory framework.

[1] Providers who place AI systems or general-purpose AI models on the market or put them into service within the EU, regardless of their place of establishment; deployers of AI systems established in the EU; distributors and importers of AI systems; product manufacturers who place on the market or put into service an AI system together with their product under their own name or trademark; affected persons located within the Union; providers and deployers of AI systems located in third countries, where the output produced by the system is used in the EU. However, AI systems and models used exclusively for military or research and development purposes, as well as natural persons using AI systems during a purely personal activity, or where the AI system is released under a free and open-source license, are excluded from the regulation's scope.

In this context, Regulation 2019/881 (**Cybersecurity Act - CSA**) has the objective of guaranteeing the effective functioning of the internal market while simultaneously attaining a high level of cybersecurity and trust within the EU. It establishes the objectives, tasks and organisational aspects of the EU Agency for Cybersecurity (ENISA) and introduces **European cybersecurity certification schemes** applicable to specific ICT products, services and processes within the Union.
A proposal to amend the CSA is currently under consideration. The proposed amendment would empower the European Commission to adopt European cybersecurity certification schemes for **managed security services** through implementing acts.

Regulation 2554/2022 (**Digital Operational Resilience Act - DORA**) came into force on 17 January 2023 and will be applicable to a wide range of financial entities starting from 17 January 2025. The DORA **extends beyond traditional financial entities**, such as banks, insurance companies and investment firms, **to encompass new actors in the financial sector**, including crypto-asset service providers and ICT service providers (e.g., cloud service providers). This framework requires businesses to also comply with a **wide range of obligations** related to governance and internal organisation, ICT risk management, incident management and reporting, digital operational resilience testing, third-party ICT service provider management, and information sharing.

On 18 October 2024, Directive 2555/2022 (**NIS2**) became fully applicable in all Member States, replacing the original NIS Directive (2016). The scope of entities subject to the provisions is expanded, replacing the previous distinction between Operators of Essential Services (OSEs) and Digital Service Providers (DSPs) with a classification into two categories - essential entities and important entities. Adopting an "**all-hazards approach**" to safeguard the EU's information and communication systems against cyber (and other) threats, the NIS2 delineates the (minimum) **security measures** that entities are obliged to implement, with a particular emphasis on the security of the **supply chain**. Furthermore, it stipulates the requisite timelines and procedures for the **reporting of incidents** that are deemed significant based on a predefined set of criteria.

Regulation 2024/2847 (**Cyber Resilience Act - CRA**) was published in the O.J. of the EU on 20 November 2024 and will be applicable in all Member States by 11 December 2027. CRA outlines **horizontal cybersecurity requirements for products with digital elements** that are intended, or reasonably foreseeable, to be used in a way that involves a direct or indirect logical or physical connection of data to a device or network. In this regard, CRA identifies those products with digital elements that are considered critical, and a **comprehensive set of obligations imposed on manufacturers, importers and distributors**. There are several **points of intersection between the CRA and the NIS2 Directive**. For example, as previously mentioned, the NIS2 Directive includes provisions for managing cybersecurity risks within the supply chain. However, it does not explicitly impose mandatory security requirements on products with digital elements, despite the fact that this is a critical area. Thus, the **CRA can be viewed as a complementary piece of the NIS2 framework**, particularly when considering that products with digital elements often serve as critical suppliers to essential or important entities under the NIS2.

Since a large part of global competition is contingent upon the capacity to keep pace with digital innovation, the European Union has been engaged for years in the formulation of strategies designed to facilitate a digital transition within Member States, thereby ensuring Europe's capacity to assume an active role in the race towards digitalisation.
Thus, Regulation 2024/1309 (**Gigabit Infrastructure Act - GIA**), which came into force on 11 May 2024, aims to enable a faster, more economical and effective deployment of Gigabit networks across the EU. It will become fully applicable in November 2025. In particular, the GIA, **acknowledging the pervasive distribution and penetration of 30 Mbps networks and their inadequacy to support new digital technologies**, seeks to implement actions that **accelerate the development of ultra-fast broadband (both fixed and mobile) and reduce associated implementation costs**. This is expected to be achieved by revising the rules for access to existing physical infrastructures, setting out elements for determining access prices and conditions for denial, as well as granting operators the right to negotiate agreements on civil works coordination and permit issuance procedures.

1.2 Entering the second half of the Digital Decade

As also highlighted in the Draghi Report, **the most wide-reaching EU laws enacted under the outgoing Commission are *ex-ante* regulations** that prohibit certain behaviours and mandate the adoption of others. As mentioned in the previous section, almost all these legal frameworks are in their implementation phase.

For example, in view of the urgency and importance of certain **AI Act** provisions, their application and enforcement have been accelerated to **2 February 2025**. This encompasses the regulation of **AI systems that present an unacceptable risk** (and are therefore prohibited, with few exceptions). As a result, **draft non-binding guidelines were issued on 13 November** to clarify the boundaries of the prohibitions and their exceptions. This document was subject to a period of **public consultation until 11 December 2024**, after which **it will be published in early 2025**[iii]. The next important deadline is scheduled for **2 May 2025** (Art. 56), when the AI Office is required to publish a **Code of Conduct** applicable to GPAI models and those that may pose a high risk to users[2]. Preparatory work has already begun, and it is envisaged that the process leading to the final Code of Conduct will be concluded by April 2025, following five plenary discussions involving all participants and interested stakeholders[iv]. In addition, to facilitate the early implementation of the AI Act, the Commission introduced the **AI Pact**, which calls for voluntary commitments from companies both within and outside the EU. The AI Office is responsible for the collection and publication of these commitments, with the aim of ensuring transparency, enhancing accountability and credibility, and bolstering

[2] This provision will enable the Commission to intervene by 2 August 2025 in the event that a code is not available or if the AI Office determines that it is insufficient to fulfil the regulatory requirements. In such an eventuality, the Commission is required to adopt implementing acts with the objective of establishing common standards for the GPAI models' providers.

confidence in the technologies developed by the organisations that have made these pledges. An interim draft was unveiled in May, shaped by the input and insights provided by stakeholders engaged with the AI Pact network. The **final version of the AI Pact issued on 25 September** has been subjected in advance to a review by the entities that have chosen to participate in the initiative (at the moment, over 130 enterprises)[v].

Another example is the **NIS2 Directive**. Where security measures (Art. 21) and the reporting of serious incidents (Art. 23) are concerned, the **Commission Implementing Regulation 2024/2690** of 17 October 2024 has been adopted[3]. It specifies the application procedures for NIS2 concerning the technical and methodological requirements for cybersecurity risk management measures and defines the cases in which an incident is considered important. It is worth noting that, **while this legal act is useful for all categories of entities falling within the scope of the NIS2 Directive, it applies exclusively to certain entities[4]**. Regarding the next steps for implementing this directive, 2025 will be a year with several important deadlines, before which Member States and entities potentially subject to the NIS2 will need to collaborate proactively. For instance, they will need to work together to establish a list of essential and important entities.

We are now entering the **second half of the Digital Decade**, to be overseen by the von der Leyen Commission II during the years 2024-2029. **Some important legal acts will have to be finalised**, such as those described below.

The proposed **ePrivacy Regulation** (COM/2017/010 final) was designed to replace the ePrivacy Directive of 2002. Still under development, even though it seems to be at a standstill, the ePrivacy Regulation seeks to protect the rights of internet users, more specifically the confidentiality of their communications. This protection covers any form of digital communication, from instant messages, emails, metadata, to cookies and IoT. It has many connections to the GDPR and some to the DA. The ePrivacy Regulation will **complement the GDPR** rules on personal data processing by providing specific rules on electronic communications and, therefore, will take precedence over the latter. **As with the DA, the ePrivacy Regulation applies to personal and non-personal data,** and relies on user consent for the processing of personal data (and the data users generate). However, while the DA gives rights to the users to choose who can access the data they generate, the ePrivacy Regulation grants individual rights related to the confidentiality of their communications.

[3] In light of the pivotal role these elements play, on 7 November, ENISA published a draft of the guidelines and initiated a public consultation process concluding on 9 December. The objective is to furnish guidance on the technical and methodological prerequisites for cybersecurity management measures under the NIS2. It is specified that, although the guidelines are directed at entities within the scope of the Implementing Regulation under review, they can be considered useful by other public or private entities with the intention of enhancing their cybersecurity position. Indeed, the document contains a mapping, augmented with use cases, which correlates the NIS2-relevant requirements with international and European sector standards, as well as elements identified in the legislation of the various MSs.

[4] (i) DNS service providers, (ii) TLD name registries, (iii) cloud computing service providers, (iv) data centre service providers, (v) content delivery network providers, (vi) managed service providers, (vii) managed security service providers, (viii) providers of online marketplaces, of (ix) online search engines, and of (x) social networking services platforms, and (xi) trust service providers.

With regard to certain AI systems, the above **Directive on liability for defective products** may have **numerous overlaps with the proposed "AI Liability Directive"** on adapting non-contractual civil liability rules to artificial intelligence (COM/2022/496 final). The EP's JURI committee requested a supplementary impact assessment study from the European Parliamentary Research Service (EPRS) on this, with the results published on 19 September 2024. In particular, **the study proposes that the scope of the AI Liability Directive should be extended to encompass general-purpose and other "high-impact AI systems"**. It is worthy of note that the study recommends a **transition from an AI-focused directive to a software liability regulation**, to prevent market fragmentation and enhance clarity across the EU.

In addition to the dossiers mentioned above, **some regulatory frameworks on digital issues that came into force in the last five years will be subject to revision**. Here, the **European Electronic Communications Code (EECC)** is a case in point. In accordance with its Article 122, the Commission is required to review the functioning of this directive and report to the EP and the Council by 21 December 2025 (and every five years thereafter). The goal of these reviews is to address the issue of uncompetitive oligopolistic market structures and to guarantee that competition in electronic communications markets continues to flourish, benefiting end-users.

Moreover, following two public consultations, on 4 July 2023, the Commission adopted a proposal for a regulation on **GDPR procedural aspects** to streamline cooperation between data protection authorities at the EU level. The starting positions of the Parliament and the Council were made public on 10 April 2024 and 30 June 2024, respectively, with the start of the trilogue negotiations scheduled for November.

Finally, another key EU legislative instrument scheduled for imminent review is the **Cybersecurity Act (CSA)**. In accordance with Article 67, the Commission is charged with evaluating the impact, effectiveness, and efficiency of ENISA and its operational procedures at the conclusion of each five-year period (for the first time, **by 28 June 2024)**. Additionally, the evaluation must ascertain whether there is a necessity to modify ENISA's mandate and, if so, what the financial implications of such a modification might be. Furthermore, the evaluation will assess the impact, effectiveness and efficiency of provisions of Title III of this regulation concerning the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improving the functioning of the internal market. Given that the Commission is required to present a report on the evaluation, including its conclusions, to the EP and the Council, while the findings of that report are to be made public, it can be stated that **the procedure is experiencing delays**.

1.3 The Letta and Draghi reports: a focus on initiatives for better EU regulation

In light of the preceding analysis of the EU digital regulatory framework, we can now consider its implications for the EU's future competitiveness. As was widely publicised, two comprehensive reports were published in recent months - the **Letta and Draghi reports**. The former addresses the completion of the internal market, while the latter focuses on the EU's waning international competitiveness. The proposals call for the **removal of obstacles** to the growth of firms, whether organic or inorganic, along with a recommendation to **reduce regulation** and to refocus **competition policy** on the expected gains from scale.

The **Letta Report**, while acknowledging the potential of the **EU Single Market** in terms of fair competition, promotion of cooperation and solidarity among Member States, also recognises **the necessity of its renewal** taking into account changes international on the international stage. Thus, the report proposes the **creation of a "European Code of Business Law"**, which it describes as a transformative step towards a more unified Single Market. This would be achieved by **providing businesses with a "28th regime to operate within the Single Market".** This initiative would directly address and overcome the current disparate array of national regulations, serving as a pivotal tool for unlocking the full potential of free movement within the EU. The proposed 28th regime would **enhance the participation of small and medium-sized enterprises in the Single Market**, enabling them to fully capitalise on the opportunities offered by the latter. Moreover, the document underscores the necessity for a strategic approach to the future of the Single Market during the legislative term 2024–2029, to facilitate **the transformation of the Single Market into a genuinely "European Market"**.

The **initial phase** entails the **comprehensive codification of the current legal framework**. However, the mere consolidation of existing legislation will not suffice to achieve a genuinely integrated European market. The codification process must be **complemented by the implementation of innovative measures and the introduction of new European instruments that are tailored to the specific needs of businesses operating within the EU**.

One such innovation is the establishment of a **"Simplified European Company",** designed to offer a more flexible and responsive legal structure for enterprises. The scope of this initiative could be extended to encompass additional areas of law where relevant, including general commercial law, market law, e-commerce law, company law, securities law, enforcement law, insolvency law, banking law, financial market law, intellectual property law, employment law, and tax law. By addressing these areas comprehensively, this initiative would equip European enterprises with the tools and structures needed to thrive in an increasingly competitive global environment.

In instances **where the EU holds exclusive competence**, it is suggested that **the European Business Code replace national laws** in order to address existing overlaps and inefficiencies. **In other areas**, the Code **would serve as a complement to national laws**, introducing new instruments that businesses may opt to utilise. While enterprises would be obliged to comply with the stipulations set forth in the Code, they would retain the autonomy to choose between novel European instruments and extant national frameworks. Consequently, **the European Business Code would provide economic actors with a "28th regime", facilitating their "Europeanisation" and positioning the Single Market as the natural horizon for business growth and development**.

The Letta Report also states that **the creation of a European Business Code is a long-term project**. Nevertheless, **several immediate measures could be implemented** to reduce the complexity of operating within the Single Market. For example, the **streamlining of administrative procedures** and the **reduction of bureaucratic burdens** are considered of paramount importance. It is of particular importance to address these challenges, given that SMEs frequently lack the resources and personnel required to navigate the complex administrative requirements of EU legislation.

Furthermore, **the Draghi Report**, published on 9 September 2024, **also emphasises these issues**. In particular, it **proposes a new industrial strategy, centred around 10 key industrial sectors**. On digitalisation, the report states that the **EU's competitiveness will increasingly depend on the digitalisation of all sectors and on building strengths in advanced technologies**, which would drive investment, jobs and wealth creation.

The report specifically analyses the root causes behind Europe's lack in innovative digital technologies, focusing on the existing regulatory framework. It highlights **the EU's regulatory approach towards technology companies, stating that this approach hinders innovation**. The report portrays a legal system that is highly complex, which **introduces a series of regulatory barriers, restrictions on data usage, and burdensome, costly, and fragmented procedures across Member States** which act as a deterrent to investment, greatly constraining the growth potential and competitiveness of European companies. The report concludes that the current regulatory environment has the effect of conferring a **competitive advantage on larger enterprises, which are better placed to bear the costs of compliance, to the disadvantage for smaller players.**

The report presents a series of overarching principles and targeted recommendations for future action. It highlights the need to prioritise the principle of **competitive neutrality in key sectors**, directing regulation towards facilitating market entry and adapting to the evolving dynamics of the economy and the pace of technological innovation. Of particular interest is the proposed approach advocating for a merger review process that considers the **impact of market concentration on the future potential for innovation in critical innovative fields**.

In accordance with the intention to conduct a meticulous assessment of the influence of regulations on market behaviour and competitive dynamics, the document identifies **two pivotal points**:

1. A comprehensive evaluation of the **influence of digital and other regulations on small enterprises, with the objective of exempting SMEs from compliance requirements that are beyond their capacity to fulfil**;
2. **Reduction of *ex-ante* regulation at the national level in favour of *ex-post* enforcement** in cases of abuse of a dominant position or other anticompetitive conducts.

In line with the goal of streamlining procedures, the document additionally recommends the harmonisation of licensing regulations and procedures across Europe, as well as the establishment of European-level auction design standards to facilitate economies of scale.

In order to further reduce the overall complexity of the situation, the report suggests the appointment of **a new Vice-President of the Commission for Simplification**, whose role would be to streamline the *acquis*[5]. The role would entail a fixed period of at least six months at the outset of each Commission's term, during which the **existing regulatory framework across economic sectors would be subjected to a comprehensive evaluation and stress-testing process**. Subsequently, a second phase would be initiated, with the objective of **simplifying the regulatory framework and eliminating redundancies and inconsistencies**. This phase would prioritise the sectors facing significant international competition. A single, unified methodology would be employed for the aforementioned impact assessments.

In line with the objective of **harmonisation**, the document further recommends the enhancement of the rules governing the **transposition of directives, with the introduction of a new standard requirement for Member States**. This would entail a systematic evaluation of new legislation employing the same methodology utilised by EU institutions. Furthermore, the report proposes a **"revamped competitiveness test"** to assess the cumulative impact of compliance costs and administrative burdens imposed by new legislation, specifically for SMEs. This test would seek to simplify and reduce reporting requirements to enhance proportionality, extending these measures to include small mid-cap enterprises.

[5] This recommendation is in accordance with the guidance set forth in the mission letter of the Commissioner for Economy and Productivity, Implementation and Simplification, Valdis Dombrovskis.

1.4 Commitments of the EU Commission

The recent hearings of the Commissioners-designate provided a valuable opportunity to take a close look at the European Commission's digital priorities for the coming mandate. In her opening speech before the Parliament, Henna Maria Virkkunen, Executive-Vice-President on Tech Sovereignty, Security and Democracy, immediately remarked that **AI, quantum, cloud, semiconductors and space will be at the centre of her mission**. The EU's strategy, she added, will follow a twofold approach: "First, we have to take all the actions to boost innovation and investments in frontier technologies; second, we need to ensure a level playing field, security and a safe online space for our citizens. Everybody who wishes to do business in Europe has to follow European rules."

The aim is to make Europe "an AI continent – the best place in the world for developing trustworthy and advanced AI" to be achieved in three steps. First, **a boost to AI computing power through the AI Factories initiative**. This initiative, to be launched within the first 100 days of the next mandate, aims to provide startups, researchers and industry with supercomputing capacity. Second, an 'Apply AI' strategy to **stimulate new industrial applications of AI** and improve public services such as healthcare. Thirdly, **an AI ecosystem in research and science** will be developed together with the Commissioner for Startups, Research and Innovation. In addition, more data sharing and access to highquality data, in line with data protection rules, will be essential for Europe to boost innovation. This will be addressed in a dedicated **Data Union Strategy**, while a **Cloud and AI Development Act will allow every business to access cloud and AI services**, which will be improved and scaled in an energy-efficient way. A quantum strategy will also be presented, including a plan for quantum chips.

Regarding connectivity, a key driver of innovation in which Europe is lagging behind its competitors, Ms Virkkunen announced that **a Digital Networks Act will be proposed to promote secure high-speed broadbands** for all, remarking on the **vital need for high standards of cybersecurity**, especially in critical sectors. Technology leakages to countries of concern must be tackled, a supply of critical telecom equipment must be secured, and concrete proposals will be presented to improve the resilience of the submarine cable infrastructure. At the beginning of next year, **the Cybersecurity Act (CSA) will be revised to enforce cyber legislation in the Member States and to de-risk high-risk vendors from the telecommunication infrastructure.**

Ms Virkkunen also expressed a strong commitment to **digital education and protection** for citizens. For example, **a Democracy Shield will be developed to protect European democracies** against electoral interference, disinformation and manipulation by malign foreign actors. Furthermore, the Commission will work to protect cultural diversity and to ensure that creators are rewarded for their work.

Finally, Ms Virkkunen stressed **the importance of reducing administrative and regulatory burdens,** also through the use of technological solutions. This will be achieved through close cooperation with Valdis Dombrovskis, Commissioner for Implementation and Simplification and for Economy and Productivity, who is responsible, among other duties, for coordinating the **reduction of red tape**

and leading the negotiations on a **renewed inter-institutional agreement on simplification and regulation**, so that new legislative initiatives will have to adhere to **better regulation guidelines.**
The incoming Commission has indeed set ambitious objectives to revitalise the EU's regulatory framework, **enhance competitiveness and digitalisation**, foster innovation, and reduce unnecessary burdens while maintaining the Union's high standards for sustainability, social fairness, and consumer protection.
Central to this vision is the creation of a more efficient and predictable regulatory environment, designed to support economic growth and ensure that the benefits of EU policies reach citizens and businesses alike. Indeed, **a key objective of the next Commission will be to reduce reporting obligations by at least 25% overall, and by at least 35% for SMEs**.

During his hearing at the European Parliament, Mr Dombrovskis stressed his commitment to:

- cutting red tape;
- stress-testing EU legislation to **remove obsolete, duplicative, redundant and inefficient rules;**
- reducing the numerous barriers that keep the Single Market fragmented and prevent SMEs from growing and expanding in Europe;
- **leveraging the potential of AI, standardisation and automation of data** to minimise regulatory burdens;
- minimising future administrative burdens by **making the new Commission's proposals "digital by default"** and "once only";
- **expanding the use of electronic platforms** to collect and share data for reporting and doing business, and take forward work on data spaces, digital wallets and other digital solutions.

These hearings and the mission letters made it clear that digitalisation is a priority for the European Commission, which aims to increase the Union's competitiveness by digitising its society, industry and administration.

Chapter 2: Strategic Investment for a Competitive Digital Future

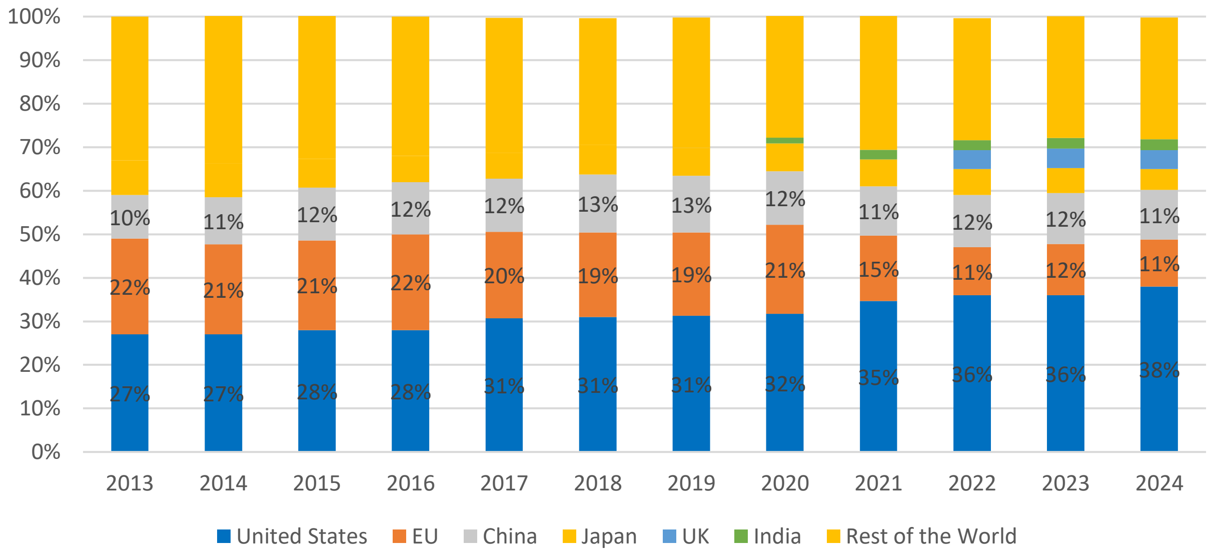
2.1 Investing in digitalisation and new technologies for a more competitive EU

Digital technologies have advanced more rapidly than any other innovation in our history – reaching around 50% of the developing world's population in only two decades and transforming societies. Not only AI, but also technologies such as supercomputers and quantum technologies, can result in numerous benefits to society as a whole.

Therefore, taking into account the potential of new technologies and the importance of the digital transformation, **the EU is determined to strengthen its digital sovereignty** and set standards, rather than following those of others, with a clear focus on data, technology and infrastructure[vi].

However, **the EU depends on third countries for more than 80% of its digital products, services, infrastructure and intellectual property (IP)**, unlike the US and China which have shifted their economic model towards ICT. From 2013 to 2024 the EU's share of global ICT revenues fell from 22% to 11%, while that of the United States increased from 27% to 38%, and China's from 10% to 11% (Fig. 2.1).

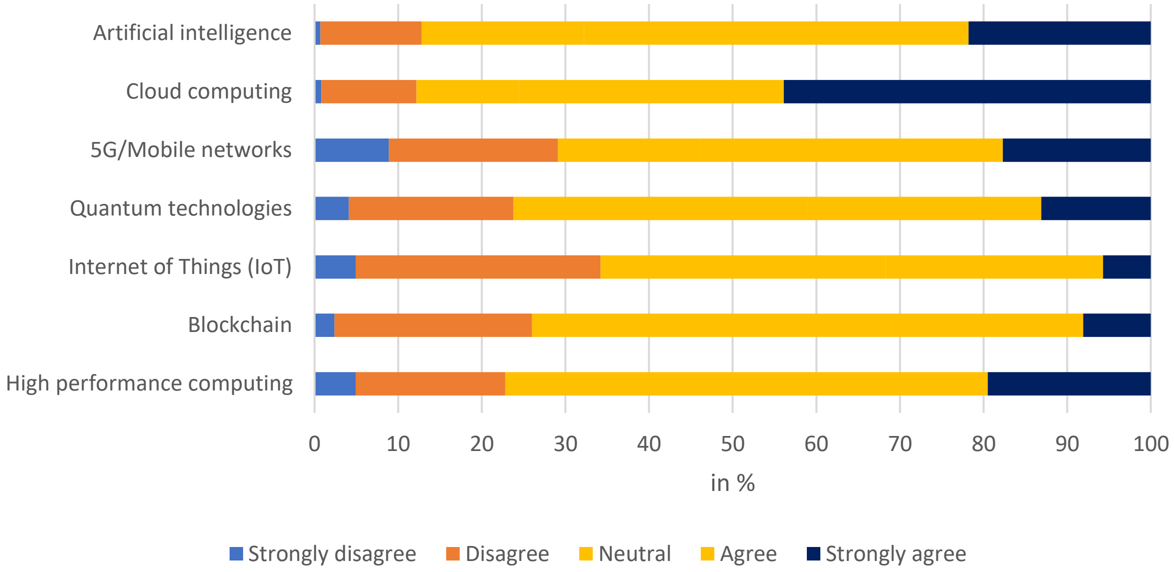
Figure 2.1: Global ICT market share 2013-2024, by country



Source: Statista (2024)

A survey conducted in 2021 by the German Council on Foreign Relations (DGAP)[vii] on over 2,500 key experts working on European technology and digital policy in government, industry, think tanks, academia, parliaments and civil society, attempted to establish a topography of Europe's perceived dependencies across key technology such as artificial intelligence, cloud computing, high performance computing and quantum technologies. The survey found that 46% of European respondents said they believe the European Union is too dependent on external players in the field of artificial intelligence. Other areas where respondents said they were concerned about the European Union's dependence on external players include cloud computing and 5G/mobile networks (Fig. 2.2). Moreover, the survey showed that the EU is perceived to depend mostly on the US compared to any other state, including China. This is particularly true in cloud computing (93% see the EU as dependent on the US) and AI (80%). On blockchain, high performance computing (HPC) and IoT, the US was seen as the primary source of dependence. Only in 5G and mobile networks did respondents identify a larger dependency on China (65%).

Figure 2.2: EU's dependency on external players in tech according to professionals



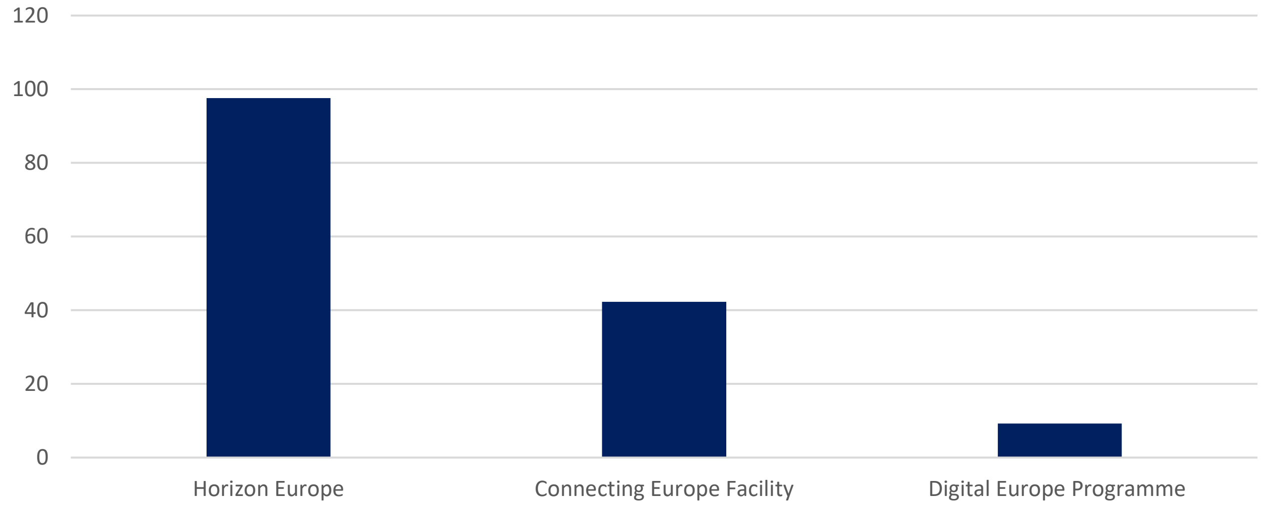
Source: DGAP Stakeholder Survey 2021

Three years later, Mario Draghi's Report[viii] also underlines the EU's excessive technological dependence. Specifically, a crucial challenge emerges from the report, namely, that without **a clear strategy of technological autonomy, the European Union risks becoming only an outlet market for technologies developed elsewhere**. Aspects such as the regulatory framework or financial support need to be thoroughly rethought to ensure that the **EU can grow independently and truly competitively**.

If the gap in development and adoption of digital technologies is the decisive factor behind the decreasing competitiveness of the EU economy, as stated in the Draghi Report, it seems obvious that the funding for digital priorities in the 2021-2027 Multiannual Financial Framework[ix] (Fig. 2.3) should be revised upwards. For instance**, the current budget of the Digital Europe Programme (less than €10 bn over 7 years) is evidently totally inadequate to fulfil the ambition of bridging the gap with the US and China.** The European Union has quite a way to go if it wants to become as competitive as the US or China. **The lack of ambition in digital investment targets contrasts with**

the overarching objective of the EU Digital Programme to build a globally competitive digital ecosystem. Therefore, the Commission should adequately define and justify the objectives and establish a comprehensive performance monitoring system for EU digital technology investments.

Figure 2.3: Planned investments in digital technologies by the EU for the financial framework from 2021 to 2027 (€ bn)



Source: Statista on EU Commission data

2.2 Artificial intelligence investments: a comparison between the EU, the US and China

Europe's growth and competitiveness are closely connected to how it will make use of data and enabling technologies such as artificial intelligence.

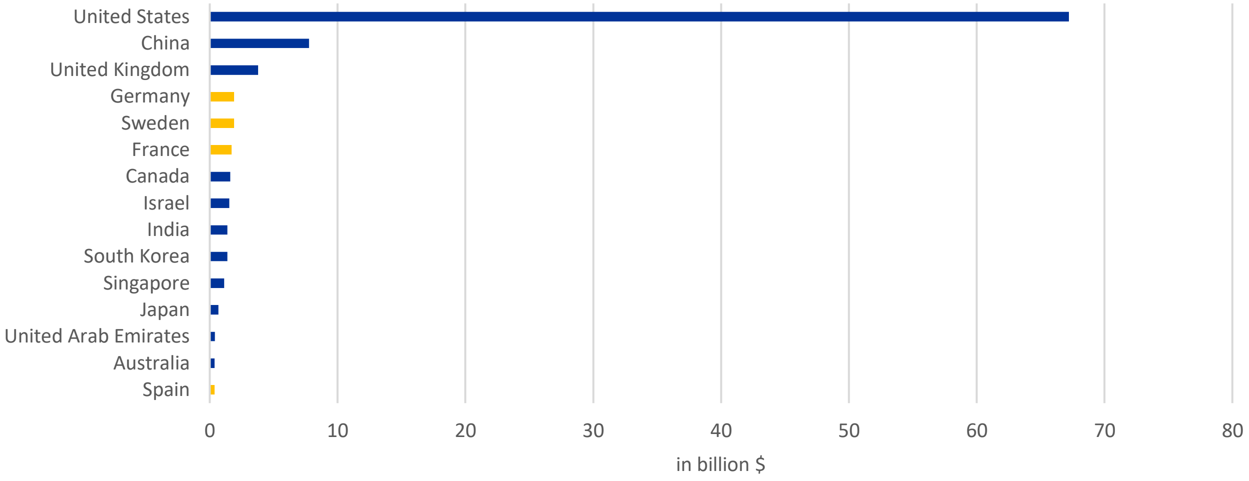
Aware of the potential of this disruptive technological frontier, the EU has stepped up its efforts to develop, deploy and promote trustworthy AI. Therefore, in June 2023, it proposed the first EU regulatory framework for AI (AI ACT) to foster the development of safe and lawful AI across the single market.

While the development of EU AI plans is broadly in line with international best practices, there are three major hindrances preventing European competitiveness - **Europe's inability to commercialise its AI development, the lack of investment, and the tension between need for data sets to train AI models and the EU's strong data protection rules that make access to data sets difficult**[x].

Looking at the data related to investment, the US was leading in financial private investment in AI startups and scaleups ($67.2 bn) in 2023, followed by China ($7.8 bn). The amount invested in AI by the US was roughly 8.7 times greater than that invested in China, and 17.8 times than in the UK ($3.8 bn). The top three EU countries in the ranking (Germany, Sweden and France) reported a total value of financial private investment in AI (about $5.5 bn), slightly higher than that recorded by the UK alone (Fig. 2.4).

The AI investment gap between the US and the EU appears to have been widening over time. In fact, while AI private investments have decreased in the EU plus the UK (-14.1%) since 2022, the US has seen a significant increase (22.1%) during the same period[xi].

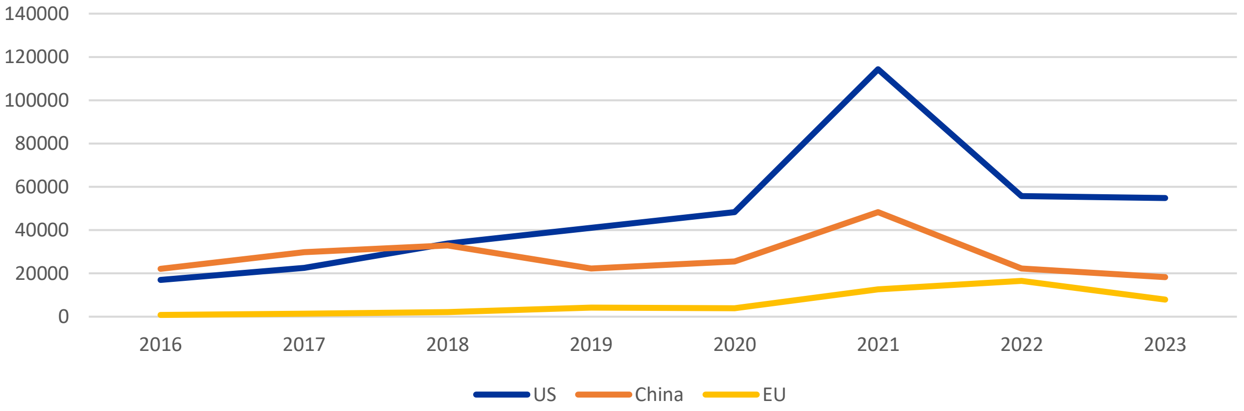
Figure 2.4: Private investment in AI by geographic area, 2023



Source: Stanford University (2024)

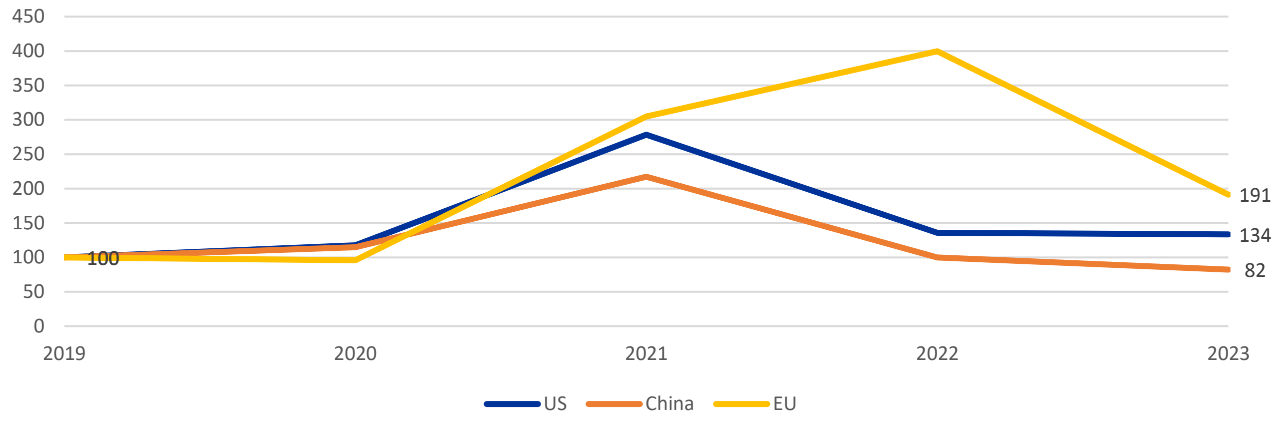
OECD data also highlights the gap between the EU, the US and China in the amount of VC investment in AI (Fig. 2.5). Although in the period 2019-2023 the EU recorded a positive trend in venture capital investment with an appreciable increase of 91% (Fig. 2.6), the difference in 2023 between the US and the EU is still staggering ($54.8 bn vs $7.9 bn, respectively).

Figure 2.5: VC investments in AI (in $ m)



Source: OECD (2024)

Figure 2.6: Trend VC investments in AI (Base year 2019=100)

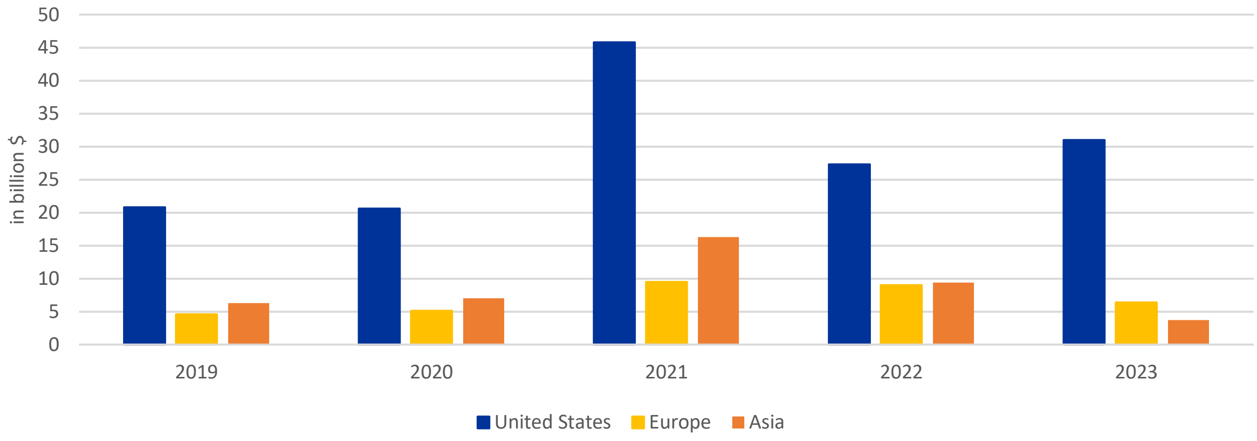


Source: I-Com elaboration on OECD data

In terms of the amount of funding for AI startups, the United States also dominates the global stage. As of 2023, they accounted for more than 50% of global funding for AI-focused startups. Europe, however, gained over Asia (Fig. 2.7).

Lower private investments weigh on the EU's competitive position and the risk is for Europe to become totally dependent on AI models designed and developed abroad.

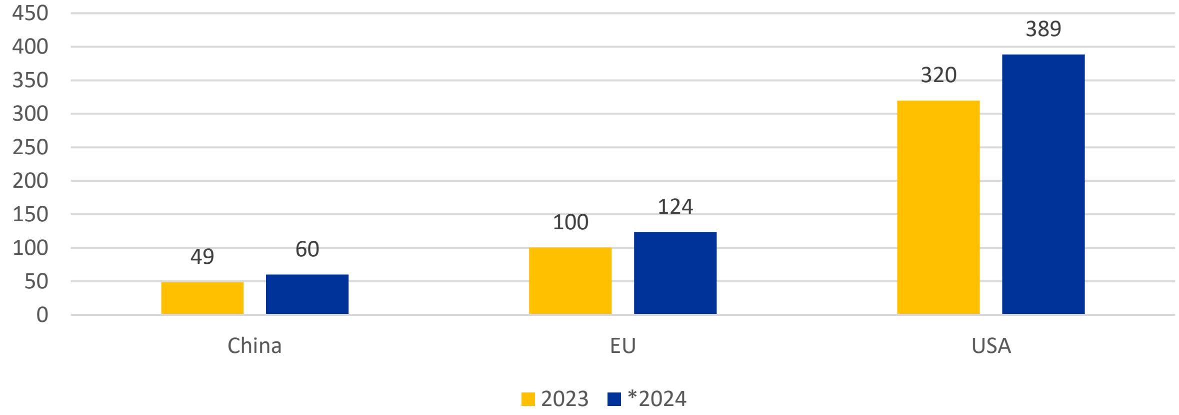
Figure 2.7: AI startup funding worldwide from 2019 to 2023, by region



Source: Statista (2024)

Moreover, Europe lags behind the United States with regard to cloud computing and the necessary infrastructure for AI. Looking at cloud market data, the US market is clearly the most important in the world, with a value of $ 320 billion in 2023, rising to $389 billion by the end of that year (+21.5%). The EU ranks second among the economies analysed, with a value of $100 billion in 2023, which could rise to $123.5 billion by the end of 2024. China, with a market value of $49 billion in 2023, appears to be the most behind, but also with the fastest growing market (Fig. 2.8).

Figure 2.8: Public cloud revenues by geographical area ($ bn)



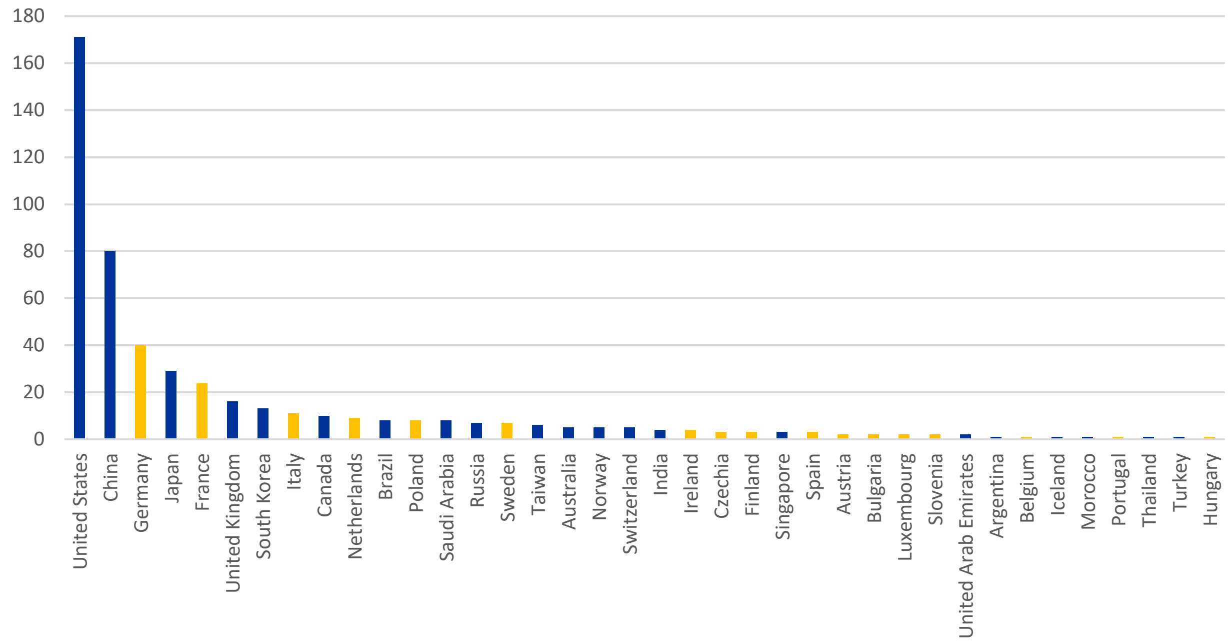
Note: Forecast data - Data up to September 2024*
Source: Statista (2024)

According to Draghi's report, **the absence of a scale comparable to US hyperscalers, EU companies will find it very difficult to enlarge their market share in cloud and invest in full platform services, and will most likely continue to depend on hosting or reselling solutions by US-based providers**. Several EU industrial alliances for cloud-based technologies and data exchanges have been created with various remits (Andromède, Gaia-X, Catena-X), but the results are so far[xii] minimal.

2.3 The role of the EU in supercomputing and quantum technologies

In 2018, the European High Performance Computing Joint Undertaking (EuroHPC JU) was established. It is a joint initiative between the EU, European countries and private partners to develop a world-class supercomputing ecosystem in Europe. The EuroHPC JU is already equipping the EU with a world-class infrastructure of pre-exascale and petascale supercomputers and the three EuroHPC pre-exascale supercomputers (Lumi, Leonardo, Marenostrum) remain in the top 10 of the most powerful supercomputers in the world.
According to the Top500 list[xiii], although North America dominates the ranking with the largest number of supercomputers in the world, **the European Union with over 100 supercomputers spread across its Member States has overtaken China** (Fig. 2.9).

Figure 2.9: Geographic distribution of the world's 500 most powerful supercomputers



Source: I-Com elaboration on TOP500.org data (June 2024)

Moreover, considering the importance of quantum technologies for the development and competitiveness of economies, **the EU Commission has launched several initiatives to make EU a world leader and a dynamic and attractive region for innovative research, business and investments in quantum**[xiv].

In 2018, the EU Commission established a large-scale research and innovation initiative known as the **"Quantum Flagship"**. Specifically, the Quantum Technologies Flagship aims to support the work of hundreds of quantum researchers over 10 years, with an expected budget of €1 billion from the EU[xv]. Its goal is to support the transformation of European research into commercial applications that make full use of the disruptive potential of quantum. It is funding projects in four core application areas - quantum computing, quantum simulation, quantum communication quantum sensing, and metrology.

Since June 2019, all 27 EU Member States have signed the **EuroQCI Declaration**, agreeing to work together, with the Commission and with the support of the European Space Agency, towards the development of a quantum communication infrastructure covering the whole EU[xvi].

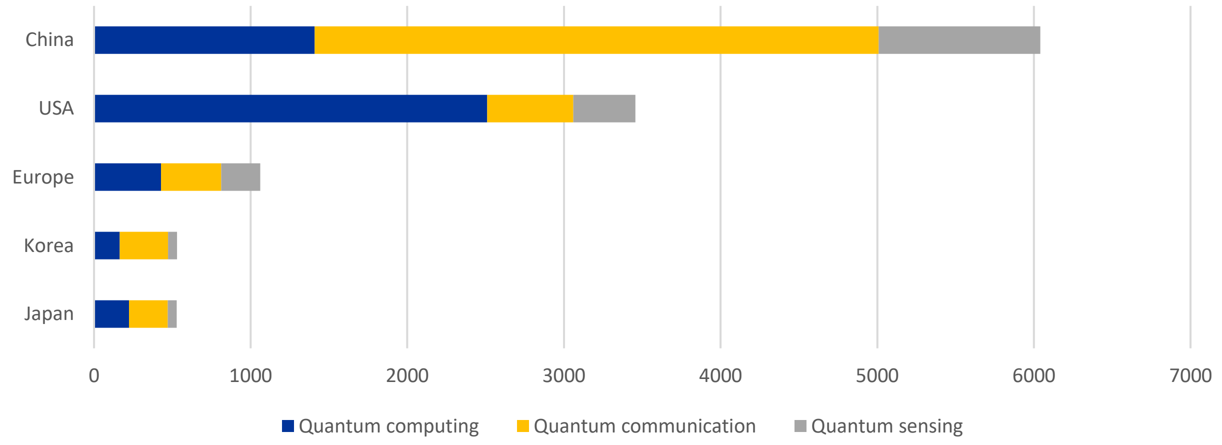
Moreover, the Digital Decade Strategy aims for Europe to have its first computer with quantum acceleration by 2025, paving the way to being at the cutting edge in quantum capabilities by 2030.

At the same time, Member States are pursuing a wide range of activities in quantum. A number of them have established or announced national quantum initiatives, testifying to their aim of leading advances in quantum research and industrial deployment, and have undertaken or are announcing major investments to this end.

The EU's commitment to quantum technologies can also be seen in **the European Declaration on Quantum Technologies**[xvii] signed by twenty-six Member States in 2023[6]. The signatory Member States recognise the strategic importance of quantum technologies for the scientific and industrial competitiveness of the EU and commit to collaborating on the development of a world-class quantum technology ecosystem across Europe, with the aim of making Europe the "quantum valley" of the world, the leading region globally for quantum excellence and innovation.

However, at the moment, looking at patents, if China dominates the scene with the largest number for quantum technologies, especially in quantum communication, the US are first in quantum computing. Europe lags behind, being ranked in third place for inventions filed, after the US and China in any of the three segments (quantum computing, quantum communication and quantum sensing)(Fig. 2.10).

Figure 2.10: Number of patent families per quantum technology, by country



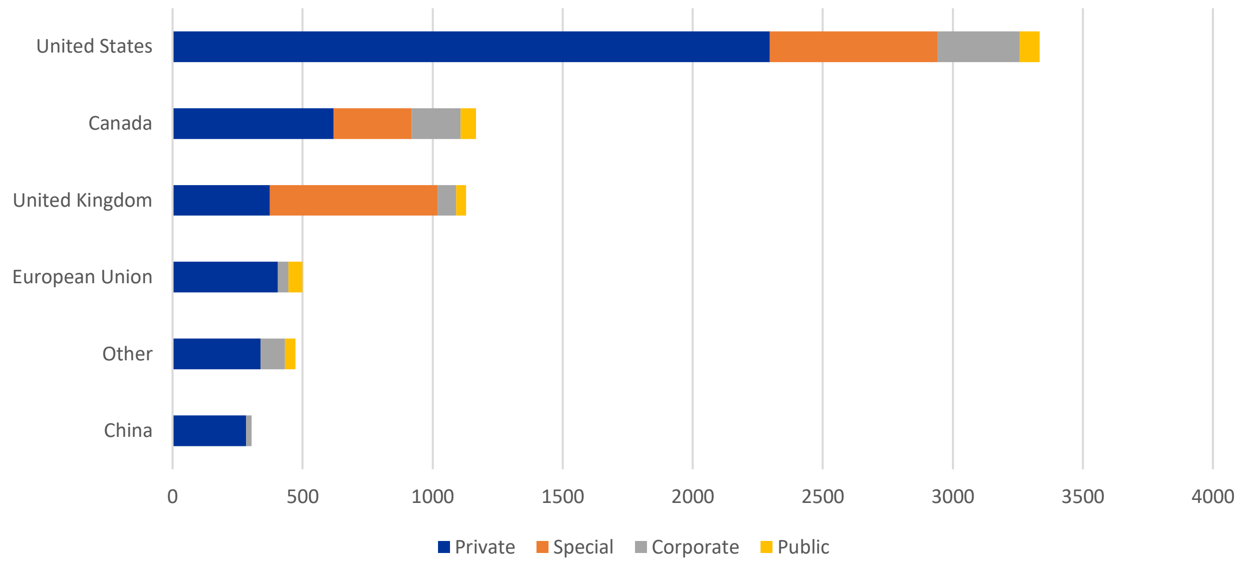
Note: data include only patent families with a first filing before 1 January 2022
Source: The Global Patent Landscape in Quantum Technologies (2024)

If for public investment, the EU ranked second only to China worldwide over the period 2001-2022 with more than $8 billion allocated (source: McKinsey, 2023), on the contrary, the European Union suffers from very limited private investments in quantum technologies compared to the other countries, especially to the US that dominates the ranking (Fig. 2.11). Moreover, according to the Draghi Report, EU firms attract only 5% of global private funding compared with the 50% attracted by US firms. China and the US, moreover, hold technological leadership in most critical components or materials for quantum computing platforms.

[6] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Spain, Slovakia, Slovenia, and Sweden.

As in the case of artificial intelligence, lower private investment weighs on the EU's competitive position and there is a risk that Europe will fall behind in quantum technologies.

Figure 2.11: Total investment in QT startups by location and primary investor type (2001–22, $ m)



Source: McKinsey (2023)

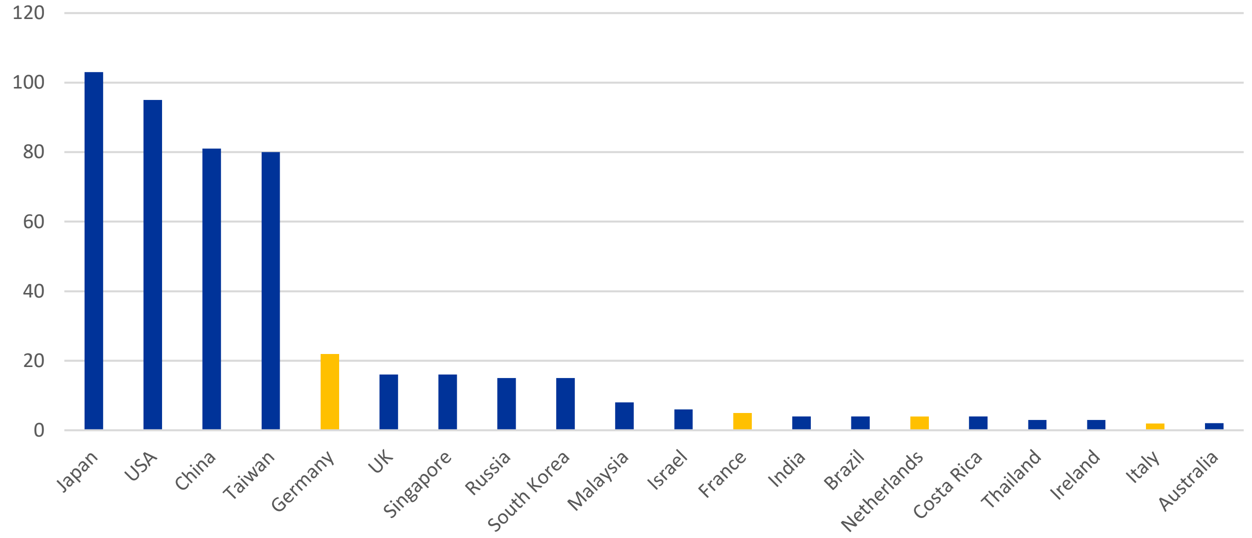
2.4 The EU's commitment to semiconductor production

The Digital Europe Programme strengthens investment in a range of areas including semiconductors. However, despite the Chips Act, overall investment and public support for semiconductor production in the EU remains below that of the US.

Around € 100 billion of total investments in industrial deployment have been announced in the EU since the proposal for a European Chips Act, but most is supported by Member States under State Aid control, with only a minimal portion of € 3.3 billion coming from the EU budget. Instead, the US CHIPS Act allocated € 52 billion in federal subsidies alone to research and manufacturing, not including state-level subsidies as well as tax credits and loans[xviii].

Certainly, the United States and China play a particularly important role in the semiconductor value chain. Analysing the main countries by number of active semiconductor manufacturing facilities, we see that the countries of East Asia and the USA clearly dominate (Fig. 2.12). The European Union has only four Member States in the top 20 (Germany, France, the Netherlands and Italy), and with considerably lower numbers than the Asian and American countries[xix].

Figure 2.12: Top 20 *countries by number of active semiconductor manufacturing facilities, 2024*



Source: World Population Review - updated to October 2024

In this scenario, the recent announcement of a pause to Intel's multibillion-dollar project in Magdeburg, Germany, is a major blow to the government of Olaf Scholz and, in general, to EU. In fact, the plant had also been seen as pivotal to EU plans to double its share of the global market from less than 10% today to 20% by 2030.

2.5 The Draghi recipe to increase strategic investment in the digital realm

The report, as part of Europe's competitiveness strategy for the coming decade, suggests policies and initiatives on digitalisation and advanced technologies, supported by significant public and private funding. It prioritises three areas: i) **high-speed/capacity broadband**; ii) **computing and AI**; iii) **semiconductors**.

I. High-speed/capacity broadband

The document highlights that regulation and competition policy in the telecom sector have **disincentivised consolidation**, favouring a multiplicity of smaller players in each national market. Furthermore, the multi-country set-up of the sector has also led to a **costly proliferation of different obligations** for EU telecom operators, with the total **number of regulators active in digital networks across all Member States exceeding 270**.

Consequently, the EU should aim to:

- boost the deployment of competitive high-speed, low-latency, ubiquitous mobile and fixed broadband services, as well as autonomous satellite capacity by 2030. These services should be delivered throughout Europe seamlessly at a standard on par with the best experiences globally;
- increase private investment in digital networks (5G standalone and fibre), supporting consolidation of players and infrastructures, and underpinning leadership in strategic areas (e.g., O-RAN, edge computing, network API standardisation, IoT and other M2M business services);
- strengthen the security and open strategic autonomy of the EU's digital communication networks by supporting EU-based providers of equipment and software for communications.

To achieve these objectives, the EU should **adopt a new "EU Telecoms Act" to set a new strategic stance on telecommunication services**.

II. Computing and AI

The EU is losing ground in R&D and in the creation of innovative tech companies with a global reach. As a result, the EU has developed few homegrown pan-EU digital platforms, and no pan-EU platform is among the most visited in Europe. However, **the EU has secured a strong international position in high-performance computing (HPC), a unique advantage to exploit in areas such as AI**, and to stimulate private investment.

For these reasons, the EU should aim to:

- secure a strong position during the next five years in AI embedded in key industrial sectors, such as advanced manufacturing and industrial robotics, chemicals, telecoms and biotech based on a set of EU-developed sectoral Large Language Models and Vertical Models;
- expand the EU's computing capability and capacity of the Euro-HPC network across Europe to serve both science and research, as well as to business ventures;
- retain control of security, data encryption and residency capabilities within EU companies and institutions and facilitate the consolidation of EU cloud providers;
- develop research excellence in quantum computing and couple EU HPC installations with quantum testing labs.

To achieve these objectives, the EU should adopt a new "*EU Cloud and AI Development Act*", aimed at enhancing European HPC, AI and quantum capabilities and infrastructure, harmonising cloud architecture requirements and procurement processes, as well as coordinating priority initiatives to scale-up private involvement and financing.

III. Semiconductors

The **EU must de-risk its strategic dependencies and improve its capabilities in semiconductors**, focusing on supply chain segments where it has or can develop a competitive advantage. The EU should aim to:

- boost R&D in selected mainstream and innovative product segments, such as larger nodes (sensors, power controls, etc.), where the EU is already present;
- develop a sovereign position in design and manufacturing processes, incentivising technology transfer only for newer manufacturing technologies;
- strengthen EU companies of demonstrated excellence in selected semiconductor equipment and materials, defending their export ambitions and expanding their addressable markets.

To achieve these objectives, **the EU Chips Act should be reviewed and expanded towards increasing funding, coordination and the speeding of public-private cooperation at continental level, as well as maximising joint efforts to strengthen innovation in semiconductors and the presence in most advanced chips segments**.

Chapter 3: Empowering SMEs: The Role of Upskilling, Reskilling, and Sectoral Dataspaces in Southern Europe

In the dynamic and interconnected global economy of the 21st century, Small and Medium-sized Enterprises form the backbone of Southern Europe's economic and social framework. SMEs not only drive economic activity but also embody the region's rich cultural and industrial diversity. Representing a significant share of employment and GDP in countries like Spain, Portugal, Italy, and Greece, SMEs are pivotal to economic growth, resilience, and innovation. However, these enterprises face mounting challenges as the region grapples with the twin transitions of digitalization and sustainability - both cornerstones of the European Union's strategic vision for the future.

The emergence of transformative initiatives such as the upskilling and reskilling programs and sectoral dataspaces offer hope. These efforts, rooted in collaboration between national governments, the EU, and the private sector, aim to address the unique challenges faced by SMEs while unlocking opportunities for growth, innovation, and global competitiveness. By equipping workforces with cutting-edge digital skills and fostering secure and transparent data-sharing ecosystems, these programs align seamlessly with overarching EU objectives such as the European Green Deal and the Digital Decade targets.

Southern Europe's SMEs are not only economic engines but also cultural stewards, preserving traditions while adapting to modern market demands. Yet, their contributions are threatened by a rapidly evolving landscape. The adoption of digital tools, advanced technologies, and green practices is no longer optional but a necessity. Failure to adapt risks obsolescence, while proactive engagement with these transitions can yield significant benefits. SMEs that embrace innovation can reduce operational inefficiencies, access new markets, and enhance their resilience against external shocks.

The European SME Strategy underscores the importance of tailored support for these enterprises. By offering access to funding mechanisms such as COSME and the European Social Fund, as well as collaborative platforms like the Enterprise Europe Network and Digital Innovation Hubs, the strategy creates a robust framework for SME growth and transformation.

The shift toward a digital and sustainable economy necessitates a workforce equipped with relevant skills. Upskilling and reskilling programs emerge as crucial tools to bridge skill gaps, especially in industries such as tourism, agriculture, and manufacturing that form the economic foundation of Southern Europe. These programs not only enhance competitiveness but also promote inclusivity, ensuring that all workers, regardless of their current proficiency, can participate in the digital and green transitions.

Complementing workforce development efforts are sectoral dataspaces, which serve as digital ecosystems designed to promote the secure sharing and collaborative use of data within and across industries. Aligned with the European Union's Strategy for Data, these frameworks facilitate seamless exchange of information, enabling stakeholders to harness the power of data for innovation and efficiency. Key sectors such as agriculture, energy, healthcare, and mobility stand to benefit immensely from these initiatives.

Despite the promise of these initiatives, significant challenges persist. The lack of adequate digital infrastructure in rural areas, regulatory complexities surrounding data sharing, and the cultural resistance to change among traditional industries are formidable barriers. Financial constraints also hinder SMEs from fully engaging with these transformative programs. However, these challenges are counterbalanced by the immense opportunities offered by EU-backed funding, sector-specific training, and the creation of collaborative ecosystems. By addressing these barriers through targeted interventions, Southern Europe can unlock the full potential of its SMEs, driving economic resilience and sustainable growth.

3.1 Upskilling and Reskilling Programs Targeting SMEs in Southern Europe

SMEs are the backbone of Southern Europe's economies, representing a significant share of employment and GDP across Spain, Portugal, Italy, and Greece. Therefore, the upskilling and reskilling of SME workforces in Southern Europe is a critical step toward achieving sustainable and inclusive economic growth. However, these SMEs face unique challenges in adapting to the digital and green transitions, both of which are pivotal for ensuring sustainable growth and global competitiveness in the 21st century. Recognizing these challenges, the European Union (EU), alongside national governments, has been spearheading a series of ambitious upskilling and reskilling initiatives tailored to the specific needs of SMEs, which align with EU objectives such as the European Green Deal[xx] and the Digital Decade[xxi] targets.

The Importance of Upskilling and Reskilling SMEs

The shift toward greener economies and the adoption of advanced digital technologies are fundamentally reshaping global markets. For SMEs, which often lack the resources of larger enterprises, these transitions pose both risks and opportunities. On one hand, failure to adapt could render many businesses obsolete; on the other hand, embracing change can unlock new markets, increase efficiency, and drive innovation. Upskilling and reskilling programs are therefore essential for:

1. **Enhancing Competitiveness**: Training employees in new technologies and sustainable practices ensures that SMEs are better positioned to compete in international markets.
2. **Promoting Innovation**: A skilled workforce is better equipped to innovate, create new products, and optimize existing processes.
3. **Sustainable Growth**: By embracing green technologies, SMEs contribute to achieving climate neutrality while reducing operational costs.
4. **Economic Resilience**: Skilled SMEs are more adaptable to market changes, reducing the risk of closures and job losses.
5. **Ensuring Inclusion**: Digital literacy and green skills training ensure that all employees, including older workers and those with limited digital skills, are included in the transition.

6. **Addressing Labor Market Gaps**: Programs align workforce capabilities with evolving market demands, addressing skill mismatches.

The European SME Strategy: A Comprehensive Framework
At the heart of these efforts lies the **European SME Strategy for a Sustainable and Digital Europe**[xxii]. This framework provides SMEs with access to essential resources, including the Enterprise Europe Network[xxiii] (EEN) and Digital Innovation Hubs[xxiv] (DIHs). These platforms serve as one-stop-shops, offering training, mentorship, and support for adopting advanced digital tools such as artificial intelligence (AI), machine learning (ML), and cloud computing. The **Enterprise Europe Network (EEN)** connects SMEs with partners, funding opportunities, and training resources, while the **Digital Innovation Hubs (DIHs)** focus specifically on equipping businesses with the tools and knowledge needed to embrace Industry 4.0 technologies. By integrating these resources with national programs, the EU ensures a holistic approach to SME development. In addition, financing mechanisms such as **COSME**[xxv] (the EU program for small businesses) and the **European Social Fund** (ESF) provide the financial backbone needed for large-scale skill development initiatives. These programs emphasize improving workforce skills in areas like digital transformation and green technologies, laying a foundation for long-term resilience.

Spain has emerged as a leader in implementing upskilling and reskilling initiatives for SMEs, leveraging both national and EU-supported frameworks. Two key programs stand out:

1. **Reskilling for Employment**[xxvi] **(R4E)**: Operating as part of a broader EU strategy, R4E aims to reskill over one million workers across Spain by 2025. The program places particular emphasis on sectors undergoing significant transformation, such as tourism, agriculture, and healthcare. These industries face unique challenges due to their reliance on traditional methods, and digital transformation is critical for their sustainability.
2. **DIS4SME Initiative**[xxvii]: Focused on digital skills, this program helps SMEs integrate data interoperability and advanced technologies into their operations. SMEs in Spain have benefited from tailored training courses in areas like AI, big data, and cybersecurity, enabling them to develop robust digital solutions for personalized services and green technologies for sustainable operations.

Spain's **Recovery and Resilience Facility** further strengthens these efforts by directing substantial investments into workforce development in digital and green skills for SME employees, particularly in industries such as healthcare, agriculture and tourism.
Portugal's approach to SME upskilling is characterized by a strong focus on sector-specific needs, particularly in energy and manufacturing. The country has embraced initiatives such as:

1. **Reskilling for Employment**[xxviii] **(R4E)**: Through this initiative, Portugal offers sector-specific labs to provide targeted training for green and digital jobs, ensuring that workers in high-impact industries are equipped with the skills needed for the transition. For instance, energy sector workers are trained in renewable technologies, while manufacturing employees learn about smart factories and IoT-enabled systems.

2. **Digital Europe Programme**[xxix]: Through this EU initiative, Portugal provides training in emerging technologies, including AI, data management, and blockchain. These efforts are critical for SMEs looking to modernize their operations and tap into global markets.

Portugal's collaboration with the **Institute of Employment and Vocational Training (IEFP)** ensures a seamless integration of national and EU initiatives. By leveraging partnerships with organizations like R4E, Portugal ensures that its workforce is prepared for future challenges.

Italy's **National Strategic Plan for Upskilling and Reskilling**[xxx] is a comprehensive approach and adopts a tailored approach to workforce development, especially in green technologies and digital innovation, focusing on the specific needs of SMEs in high-priority sectors like energy and manufacturing. Key features of the strategy include:

1. **Custom Training Paths**: Recognizing that one-size-fits-all solutions are ineffective, Italy offers customized training programs for SMEs. These programs cover areas such as cloud computing, AI, and sustainable technologies, enabling businesses to address their unique challenges.
2. **DIS4SME Initiative**: Italy's participation in DIS4SME highlights its commitment to equipping SMEs with cutting-edge skills. Short-term courses on AI, data analytics, and cybersecurity are particularly popular among Italian SMEs.

By aligning these efforts with the **EU Pact for Skills**[xxxi], Italy ensures that its workforce development initiatives are consistent with broader European objectives. Additionally, Italy's focus on green technologies underscores its commitment to achieving the goals of the European Green Deal.

Greece faces unique challenges in upskilling its workforce, including geographical fragmentation and disparities in digital literacy. Despite these obstacles, the country has made significant strides through initiatives such as:

1. **DIS4SME Initiative**: Greece's involvement in DIS4SME has enabled it to provide targeted training in areas like data management, AI, and cybersecurity. These skills are essential for navigating the twin transitions of digitalization and sustainability.
2. **Pact for Skills**: Through its participation in this EU-wide initiative, Greece ensures that SMEs have access to resources and training programs aligned with European standards.

Greece's efforts are further supported by its participation in EU-wide efforts[xxxii] that prioritize SMEs in sectors such as agriculture, shipping, and tourism. These sectors, which are central to Greece's economy, are being transformed through the adoption of smart technologies and sustainable practices.

Challenges and Opportunities

Small and medium-sized enterprises (SMEs) in Southern Europe are pivotal to the region's economic and social fabric, but they face a range of **challenges** in their efforts to upskill and reskill their workforce. A major barrier for many SMEs in Southern Europe is the **lack of digital literacy** within their workforce. Employees in traditional sectors such as agriculture, tourism, and manufacturing often lack the foundational skills necessary to adopt advanced technologies like artificial intelligence (AI) and big data analytics. This gap slows the uptake of digital tools, hindering productivity and innovation. In addition, southern Europe experiences **disparities in digital infrastructure**, particularly in rural and less developed regions. Limited access to high-speed internet and advanced technological facilities makes it challenging for SMEs to engage in digital training programs, further widening the digital divide.

While programs like COSME and DIS4SME provide funding support, many SMEs face **financial barriers** as they lack the resources or knowledge to navigate the application processes for these grants. Additionally, small-scale businesses often find it difficult to allocate budgets for workforce training, given competing priorities like operational costs. Moreover, many SMEs are discouraged by regulatory and administrative hurdles. Complex administrative requirements and slow bureaucratic processes deter SMEs from participating in training programs or accessing funding opportunities. In some cases, overlapping regulations between national and EU frameworks exacerbate confusion and reduce program efficacy. Lastly, traditional businesses, especially those with long-standing operational methods, often **resist transitioning** to digital or sustainable practices. This cultural inertia limits engagement in upskilling initiatives, particularly in sectors like agriculture and artisanal manufacturing.

While SMEs in Southern Europe face significant hurdles in workforce upskilling and reskilling, the **opportunities** far outweigh the challenges. **Programs tailored to the unique needs of sectors** like energy, tourism, and agriculture can address skill gaps effectively. For instance, digital tools in agriculture -such as precision farming and IoT devices- offer immense potential to enhance productivity while promoting sustainability. **EU financial mechanisms** such as COSME, the European Social Fund (ESF), and the Recovery and Resilience Facility provide critical resources for SMEs to invest in workforce training. These programs not only reduce financial barriers but also incentivize businesses to adopt cutting-edge technologies and sustainable practices.

Partnerships between public institutions, private enterprises, and educational organizations are creating **collaborative ecosystems** and fostering innovation hubs that facilitate training and knowledge exchange. Digital Innovation Hubs (DIHs) and networks like the Enterprise Europe Network (EEN) play a crucial role in connecting SMEs with resources and expertise. In addition, the emphasis on green technologies under the European Green Deal creates **new market opportunities** for SMEs that embrace sustainable practices. Training programs focused on renewable energy, circular economy models, and eco-friendly product design can position businesses as leaders in emerging green markets. Furthermore, southern European countries are increasingly leveraging regional collaborations to share best practices and pool resources. Initiatives like Reskilling for Employment (R4E) provide a platform for SMEs to access training and tools developed across the EU.

3.2 Sectoral Dataspaces in Southern Europe

Sectoral dataspaces are specialized frameworks designed to promote the secure, transparent, and sovereign sharing of data within and across specific industries. Sectoral dataspaces represent a cornerstone of the European Union's **Strategy for Data**[xxxiii] to drive digital transformation and foster economic innovation while upholding European values of privacy, transparency, and trust. These initiatives enable secure and efficient data sharing across industries, connecting businesses, governments, and citizens in new and meaningful ways. By facilitating cross-border data exchange and collaboration between public and private sectors, dataspaces create opportunities to enhance competitiveness, drive technological advancement, and promote sustainable development in critical sectors such as agriculture, energy, healthcare, and mobility. Key objectives of sectoral dataspaces include:

1. **Enhancing Competitiveness**: By enabling businesses to access and leverage shared data, dataspaces drive innovation, efficiency, and competitiveness.
2. **Facilitating Collaboration**: Cross-border and cross-sector partnerships are encouraged, breaking down silos and fostering a collaborative ecosystem, creating a unified digital economy.
3. **Promoting Sustainability**: Dataspaces play a crucial role in optimizing resources, reducing waste, advancing green technologies, and contributing to the EU's climate goals.
4. **Empowering Citizens**: Through initiatives like the **European Health Data Space (EHDS)**, enhance healthcare delivery and empower citizens through better access to information to make informed decisions while ensuring their data sovereignty.

The **Gaia-X initiative**[xxxiv] is central to the EU's efforts, providing a framework for federated and secure data infrastructure, which promotes data sovereignty and cross-sector collaboration. By fostering interoperability and trust, Gaia-X sets the stage for the development of dataspaces in key industries across Europe.

Spain is at the forefront of sectoral dataspaces, with notable efforts in mobility, agriculture, and healthcare. These initiatives are largely driven by Spain's participation in the **Gaia-X initiative** and the establishment of a national Gaia-X hub[xxxv], which focuses on fostering data ecosystems in sectors like sustainable mobility, agriculture, and healthcare. Key initiatives in Spain include:

1. **European Mobility Data Space**[xxxvi] **(EMDS)**: Spain is a leading contributor to the EMDS, which aims to revolutionize transport systems through integrated, cross-border data-sharing solutions. This initiative facilitates the development of intelligent transport systems, including real-time traffic management, connected vehicles, and sustainable urban mobility.
2. **Sustainable Agriculture**: Through its Gaia-X hub, Spain is fostering dataspaces that support precision agriculture. By leveraging IoT devices and big data analytics, farmers can optimize crop yields, reduce resource consumption, and enhance sustainability.
3. **Healthcare Data Ecosystems**: Spain's involvement in the **European Health Data Space**[xxxvii] **(EHDS)** aims to improve healthcare outcomes by enabling secure access to medical data. This

data-sharing empowers healthcare providers to deliver personalized treatments and enhances cross-border research on diseases and pandemics.

Spain is also a member of the **International Data Spaces Association**[xxxviii] **(IDSA)**, which fosters the development of trustworthy data ecosystems. By aligning with IDSA's principles, Spain ensures that its dataspaces adhere to international standards of security and data sovereignty.

Portugal has emerged as a regional leader in leveraging sectoral dataspaces to address critical challenges in energy, agriculture, and healthcare. The country's active participation in the **Gaia-X initiative**[xxxix] and the **International Data Spaces Association (IDSA)** underscores its commitment to digital transformation and innovation. Portugal's key initiatives include:

1. **Energy Dataspaces**: Portugal is at the forefront of developing dataspaces for the energy sector. These frameworks enable real-time monitoring of energy production and consumption, fostering the integration of renewable energy sources. By supporting smart grid technologies, these dataspaces contribute to the EU's goals of carbon neutrality and energy efficiency.
2. **European Health Data Space**[xl] **(EHDS)**: Portugal's involvement in the EHDS reflects its focus on enhancing healthcare through data-driven solutions. The country is developing platforms that allow for seamless data sharing between healthcare providers, researchers, and patients, ensuring better diagnostics, treatments, and public health outcomes.
3. **Agriculture and Manufacturing**: In collaboration with Gaia-X, Portugal is fostering dataspaces that integrate advanced technologies like AI and blockchain into agriculture and manufacturing. These efforts aim to improve supply chain transparency, reduce waste, and enhance productivity.

Portugal's strong focus on collaboration is evident in its partnerships with universities, government agencies, and private enterprises. Through the IDSA, Portugal promotes digital literacy, knowledge-sharing and innovation in ICT, ensuring that dataspaces deliver tangible benefits to businesses and citizens alike.

Italy's approach to sectoral dataspaces is characterized by its emphasis on mobility, energy, and manufacturing. These sectors align closely with the EU's priorities for achieving a sustainable and digitally connected economy. Italy's key initiatives include:

1. **European Mobility Data Space**[xli] **(EMDS)**: Italy plays a critical role in the EMDS, focusing on the development of interoperable data infrastructures for cross-border transport systems. These efforts support smart logistics, reduce traffic congestion, and promote sustainable mobility solutions.
2. **Energy and Manufacturing Dataspaces**: Italy is heavily involved in creating dataspaces that enhance industrial efficiency and promote the adoption of green technologies. By integrating IoT, AI, and blockchain, these frameworks support Italy's transition to a circular economy.
3. **IDSA Collaboration**: Through its active participation in the IDSA, Italy ensures that its dataspaces adhere to international standards of data security and interoperability. This

collaboration fosters trust among stakeholders and accelerates the adoption of data-driven solutions.

Italy’s investments in sectoral dataspaces not only enhance its industrial competitiveness but also contribute to broader EU objectives such as the Digital Decade targets and the European Green Deal.

Greece faces unique challenges in its digital transformation journey, including economic constraints and regional disparities. Nevertheless, the country has made significant progress through its involvement in the **Gaia-X initiative**[xlii] and other EU-backed programs. Key initiatives in Greece include:

1. **Smart Agriculture**: Greece’s focus on agricultural dataspaces aims to modernize its traditional farming practices. By incorporating data-driven solutions such as precision farming and crop monitoring, these initiatives enhance productivity and sustainability.
2. **Renewable Energy Management**: Through energy dataspaces, Greece is advancing its renewable energy sector by optimizing resource allocation and improving grid management. These efforts align with the EU’s climate goals and support Greece’s transition to a low-carbon economy.
3. **Research and Development**: Greece’s participation in the IDSA, particularly through academic institutions like the University of Patras, underscores its commitment to advancing cutting-edge research in data technologies. This collaboration fosters innovation and accelerates the adoption of data-driven solutions across sectors.

Greece’s involvement in Gaia-X and IDSA highlights the importance of cross-border cooperation in overcoming national challenges. By leveraging European frameworks, Greece is bridging its digital divide and unlocking new opportunities for growth.

Challenges and Opportunities

Southern Europe is progressing rapidly in the development and adoption of sectoral dataspaces, driven by the European Union’s strategic focus on fostering data-driven innovation. However, despite the promising advancements, several challenges must be addressed to unlock the full potential of these transformative ecosystems. Simultaneously, the opportunities offered by sectoral dataspaces highlight their critical role in ensuring sustainable economic growth and competitiveness across industries.

Many regions in Southern Europe, particularly rural and less economically developed areas, **lack the necessary digital infrastructure** to support the effective implementation of dataspaces. High-speed internet, cloud storage facilities, and robust cybersecurity measures are foundational for dataspaces but are unevenly distributed across the region. This disparity creates a digital divide that hampers participation from smaller and rural-based enterprises. In addition, there are **regulatory and legal barriers** as the relevant frameworks for data sharing remain inconsistent across Southern Europe, creating significant hurdles for cross-border collaboration. Issues such as data privacy, intellectual property rights, and compliance with the General Data Protection Regulation (GDPR) complicate the development of interoperable dataspaces. The lack of harmonized standards makes it challenging for businesses to engage in secure and trustworthy data exchanges.

Moreover, a **lack of digital literacy** among many businesses and workers in Southern Europe further impedes the adoption of dataspaces. SMEs, which form the backbone of the region's economy, often struggle to understand and integrate advanced data technologies into their operations, limiting their ability to benefit from dataspaces. Lastly, many traditional industries in Southern Europe are slow to embrace data-driven innovation due to **cultural resistance and organizational inertia**. Sectors like agriculture and manufacturing often rely on established practices and are wary of adopting new technologies, delaying the adoption of sectoral dataspaces.

While these challenges pose significant hurdles, the opportunities presented by sectoral dataspaces in Southern Europe are transformative. Sectoral dataspaces offer unprecedented **opportunities for innovation** by enabling secure and efficient data sharing among diverse actors within industries. By pooling data resources, businesses can develop smarter products and services, optimize supply chains, and enhance customer experiences. For instance, in the **agriculture sector**, dataspaces facilitate the exchange of data on precision farming techniques, enabling farmers to improve crop yields while minimizing environmental impact. Furthermore, in the **energy sector**, dataspaces play a **critical role in green transition** by supporting the integration of renewable energy sources and smart grids. By sharing real-time data on energy production and consumption, stakeholders can optimize resource allocation, reduce waste, and accelerate the transition to a low-carbon economy. This aligns with the EU's climate goals and the European Green Deal.

Sectoral dataspaces can also **enhance competitiveness**, by enabling cross-border collaboration, dataspaces position businesses in Southern Europe to compete in global markets. For example, the **European Mobility Data Space** facilitates the development of intelligent transport systems, enhancing the efficiency and sustainability of transportation networks across the region. Moreover, sectoral dataspaces ensure that **data sovereignty** is maintained, allowing businesses to retain control over their data while benefiting from collaborative ecosystems. This is particularly critical for industries handling sensitive information, such as healthcare, where dataspaces like the **European Health Data Space (EHDS)** enable secure data sharing to advance medical research and improve patient care. Finally, dataspaces can empower SMEs by providing access to advanced tools and insights that were previously out of reach. By participating in sectoral dataspaces, smaller enterprises can leverage shared resources to innovate and grow, leveling the playing field with larger competitors.

Chapter 4: Priorities for the international agenda of EU’s digital policy in the 2024-2029 mandate

4.1 Lessons from last mandate over the 2019-2024 period

Lessons from the last European Commission’s mandate (2019-2024) show that the international engagement of the European Union institutions in technology policy with third partners has largely increased. The institutionalization of dialogues with other countries has been translated into structured platforms for trust and information exchange and, in some cases, for joint decisions on implementation roadmaps. This is the case of the EU-US Trade and Technology Council, the EU-India Trade and Technology Council, the Digital Partnership Agreements with many Indo-Pacific countries -Japan, Republic of Korea, and Singapore-, the launch of the EU-LAC Digital Alliance, or the strengthening of the Digital Agenda for Western Balkans.

Also, this mandate witnessed the first-ever coordinated support from the 27 Member States to digital diplomacy through the endorsement of the Conclusions from the Council of the EU in July 2022 on establishing a framework of digital diplomacy which serves as umbrella to coordinate all actions related to the foreign policy of EU’s technology policy. This includes security issues -e.g. the negotiations of the Framework for Responsible State Behavior on cyber norms at the UN-, economic topics -e.g. investments from the Global Gateway onto third countries, or agreements on telecommunications, 5G and others in third partners- and in regulatory convergence efforts -e.g. the establishment of the EU’s Office in San Francisco singularly devoted to giving outreach to the digital policy legislative files.

However, if the European Union’s perspective has been focused on sovereignty and open strategic autonomy since 2019, the new mandate in 2024 kicks off with a paradigm shift towards **economic security**. Also, a second layer of this transformation is marked by the transition from a regulatory focus into a **new approach oriented to industrial policy, public intervention and competitiveness as the vertebral axis of digital and clean transitions and a stronger defense baseline.**

These transformations over the 2019-2024 period have contained an international angle. This chapter addresses four main policy angles that the new mandate for the 2024-2029 period should include in the international dimension of EU’s digital policy:

(a) The institutional and governance dimension with the creation of first-ever Executive Vice-President for Technology Sovereignty, Security and Democracy;
(b) The strengthening and further coordination of digital diplomacy efforts;
(c) The technological dimension in the Enlargement Policy mostly with candidate countries to access the European Union;
(d) Revamped agenda with priority-setting and an action-based roadmap for putting the Economic Security Strategy into practice.

4.2 Boosting policy needs from Draghi and Letta reports

While both Draghi and Letta reports largely touch upon domestic policy needs at the EU level and across Member States, the international angle is present both explicitly and implicitly.

Concretely, main ideas showcase that the key driver of the rising productivity gap between the EU and the US has been digital technology. The EU failed to capitalize on the first digital revolution led by the Internet in the 1990s. At present times, high-technology capital is concentrated in the United States (e.g. 70% of foundational AI models are developed in the U.S., 65% of European cloud market is led by three U.S. hyperscalers, and 5 out of top 10 quantum-related companies are concentrated in the U.S. and four in China).

The Draghi report[xliii] indicates that the EU has lagged behind too far. However, while first-tier leadership is not possible for many technologies, the EU has the opportunity to maintain a foothold in specific areas where either the dependencies may be partially reduced or where it may become a frontrunner if investments are effectively allocated. This is the case of "sovereign cloud" solutions, where Draghi calls for further security and encryption. Selected segments are autonomous robotics, where the EU hosts around 22% of worldwide activity, and AI services such as predictive analytics, forecasting, optimization, failure detection, business intelligence and business functions.

For this to happen, Draghi recommends scalability in the spending of R&I and shifting the focus towards breakthrough innovation. It compares it to the U.S. Defense Advanced Research Projects Agency (DARPA) and other "ARPA-style" agencies. Another recommendation is the creation of stronger innovation clusters, where out of the 10 top global hubs, 4 are located in the U.S. and 3 in China. Also, looking at the international angle, Draghi proposes following a model closer to the U.S. or China for mobile network operator groups, which are concentrated in these two cases, while in the EU there are 34 groups. Fragmentation hinders competitiveness.

As for Letta, his report "Much more than a market"[xliv] provides an innovative approach to the international agenda of the EU. Only by means of a 5th freedom on research, innovation, data, competences, knowledge and education, a European integration -and, then, a coordinated EU's position worldwide- will be feasible. Under this framework, the EU will be better suited to position itself not only as a global leader in setting international standards for innovation and knowledge diffusion, but also as a creator and producer of new technologies.

These messages also translate the idea that a more integrated EU across its 27 Member States in the digital space also leads to a stronger EU's international agenda.

4.3 Institutionalization of the international dimension of EU's digital policy: the new College

The profile creation of the first-ever **Commissioner-designate for Tech Sovereignty, Security and Democracy (with an Executive Vice-President role) should put digital diplomacy at the center of its international engagement roadmap**. Mission letter[xlv] from the President of the European Commission, Ursula Von der Leyen, asks Henna Virkkunen to boost productivity with digital technology diffusion, strengthen EU's digital competitiveness, intensify investments concerning the next wave of frontier technologies -in particular, quantum computing, supercomputing, semiconductors, the Internet of Things, genomics, space technology and beyond-, and requests a long-term EU Quantum Chips plan.

Due to the limited capacity in resources, technical maturity and competitive market players on EU soil, the Commissioner-designate should channel these developments through international engagement initiatives with key partners, **identified based on the level of mutual benefit and strategic interest,** by ensuring these partnerships are sustainable and based on a level-playing field.

Also, the new EVP for Tech Sovereignty should **ensure coherence and complementarity between internal and external digital policies, especially when touching upon sensitive security-related issues**. This should apply to bilateral partnerships and to current efforts leading to global digital governance. The first case should delve into leveraging the EU's current efforts in certain technology verticals and find trusted partners. Semiconductors cannot be developed only and exclusively in the EU or in any other region. The EU should leverage the budget derived from the Chips Act and the tools from the Chips Joint Undertaking (including pilot lines and process capabilities development) to arrange collaboration arrangements with third countries.

One of the first deliverables from the EU-Japan Digital Partnership Council was a Memorandum of Cooperation establishing cooperation in semiconductors, including an early warning mechanism for the semiconductor supply chain; research and development for semiconductors; advanced skills for the semiconductor industry; use cases of semiconductor applications; and subsidy transparency. On the EU side, all collaborative research actions will be funded by the EU's Research & Innovation programme Horizon Europe including the actions launched through the Chips Joint Undertaking. In the case of the Republic of Korea, the first bilateral Forum for Semiconductor Researchers took place. The EU-India Trade and Technology Council led to the first Memorandum of Understanding on semiconductors. Also, the EU-US TTC established an early warning system for supply chain crisis in semiconductors.

However, this new mandate should broaden the scope of collaboration -from the current information exchange, R&D and early warning mechanism- towards a more ambitious agenda where joint investments may be leveraged.

Another area to ensure complementarity and coherence among internal and external actions is AI. In this case, the **AI Office should consolidate its international relations branch** with staff teaming up for engagement in concrete, tangible areas of AI technical development with third countries. Networking with other AI Offices and Safety Institutes from trusted partners and arranging priority lists will be fundamental to ensure the sustainability of technical partnerships (beyond regulatory dialogues). It is in technical development where actual leadership may take place due to the increasing integration of AI into non-technological sectors.

Also, the EVP should work on the **security angle of AI** to ensure international binding agreements on meaningful human control over the critical functions of systems deployed in defense with AI.

The second case on international governance relates to tangible actions such as the **implementation roadmap of the UN-led Global Digital Compact** where the EU has influenced the final content of the document to promote a human-centric vision. Spain has become one of the co-facilitators to ensure this implementation and the EU should play an active role. Also, **international ICT standard-setting bodies** should be a targeted area of the new Commissioner and EVP in order to enhance EU coordination. This is key to **reducing dependencies and strengthening the capacity in critical technologies**. The EU Observatory on Critical Technologies may broaden its scope and address potential policy research on which critical technologies the EU should partner up with specifically with targeted countries. For instance, the Republic of Korea and Japan have developed guidelines of National Core Technologies for basic research, and this might become an area of cooperation, falling back on the EU's Digital Partnership Agreements with each respectively.

Similarly, topics that have received little attention from an EU-wide perspective and a governance approach should be strengthened by the new College. This is the case of **subsea cable infrastructure**, for which the European Commission released a Recommendation for its security and resilience, and proposed greater coordination, unified technical cooperation, and increased funding.

4.4 Encouraging and entrusting digital diplomacy efforts

While international digital partnerships have been created rapidly during the 2019-2024 mandate with third countries and regions, as stated above, the release of the Conclusions of the Council of the EU on Digital Diplomacy[xlvi] in July 2022 signaled the high-level importance that this topic had, not only by the EU institutions, but also by the **support from each of the 27 Member States.**

With the goal to work towards a more concerted European approach, the agreement foresees **four actionable pillars: strategic objectives, core proposals, implementation mechanisms, and institutional enhancements**. While some of them have been put into motion, still most need to reach institutional maturity and further coordination in the coming years.

As for the strategic objectives, the EU should aim to position itself as a global leader in digital diplomacy by championing a human-centric and rights-based approach to technology. It is essential for the EU to leverage its geopolitical influence to shape digital governance frameworks that promote universal human rights, uphold the rule of law, and strengthen democratic principles in the digital sphere. Additionally, the EU should prioritize enhancing digital sovereignty by reducing vulnerabilities and critical dependencies in emerging and foundational technologies, ensuring resilience against external pressures.

As for the core proposals, the EU should comprehensively integrate digital diplomacy into its external action. This involves aligning digital diplomacy initiatives with existing policies, such as Green Diplomacy and Cyber Diplomacy, to address hybrid threats, cyberattacks, and foreign disinformation campaigns cohesively. The EU should foster international collaboration by partnering with global entities such as the United Nations, G7, OSCE, and WTO to uphold democratic standards and advocate for a stable, open, and secure internet governed by multi-stakeholder principles. It should also take a leading role in influencing the development of ethical technology standards through its strong presence in global standardization bodies.

The EU should actively promote its internal digital policies globally, ensuring that its regulatory frameworks, such as the "Digital Compass" vision for 2030, gain international traction. Advocacy for governance approaches that balance innovation with ethical and responsible use of technology should remain a central pillar. Another priority should be to facilitate a sustainable digital transition by utilizing digital tools to advance the UN Sustainable Development Goals (SDGs), address climate change, and build resilient digital infrastructures, particularly in regions with significant technological disparities.

To counter malicious activities in the digital sphere, the EU should strengthen its policies to combat cyberattacks, disinformation, and state-sponsored interference. Mechanisms like the Cyber Diplomacy Toolbox should be further developed and deployed, alongside initiatives to address online hate speech and violent content. These efforts will safeguard democratic processes, foster public trust, and protect the digital ecosystem from misuse.

Regarding implementation mechanisms, the EU should focus on building and strengthening partnerships to implement its digital diplomacy goals effectively. Existing collaborations, such as the EU-U.S. Trade and Technology Council, should be expanded to advance shared objectives. Additionally, the EU should integrate investments in digital infrastructure with the strategic promotion of technological solutions and regulatory convergence through digital economy packages.

The EU should engage with a broad range of stakeholders, including academia, civil society, and the private sector, to develop innovative solutions to address challenges such as data security and privacy. Promoting ethical European business practices and data governance models globally will allow the EU to set a strong example and enhance its influence in shaping digital policies.

As for institutional enhancements, the EU should invest in capacity building and institutional development. Training diplomats in digital diplomacy will enhance technical expertise and enable strategic geopolitical positioning. Regional digital diplomacy hubs within key EU delegations should be established to streamline efforts and strengthen outreach. Additionally, the EU should develop robust mechanisms for monitoring global technological developments, enabling it to address their implications for digital sovereignty and security effectively. Regular reporting and assessment of the impact of digital technologies on democracy and human rights should ensure alignment with core EU values.

Also, external factors such as the U.S. elections should be observed in order to guarantee that the EU-US Trade and Technology Council keeps on track and serves as a tangible platform to provide specific measures and joint cooperation areas. Trust is needed to ensure technological competitiveness within the EU and outside with third partners.

4.5 Enlargement and EU candidate countries

Candidate countries for accession to the EU should be a relevant element of EU's digital diplomacy efforts. Many countries have moved forward in the compliance with the required elements by the EU to enter into the process of being considered as candidate countries, such as Ukraine, Georgia or Moldova, among others.

Convergence and coherence in digital policy issues, including telecommunications, technical standards, cybersecurity certification schemes, electronic communications, or the transmission of personal data, are areas where the EU should get involved further, not only from a domestic policy perspective, but also through the lens of foreign policy. Candidate countries are also affected by **third partner's interference** in some areas such as disinformation or are **particularly vulnerable in assets such as cables or data centers' security and resilience**. The EU's international engagement should focus on making sure these vulnerabilities are overcome and there is no harmful influence from illiberal countries.

Currently, candidate countries are Albania, Bosnia and Herzegovina, Georgia, Moldova, Montenegro, North Macedonia, Serbia, Turkey and Ukraine. According to the **2024 Communication on EU Enlargement Policy**[xlvii], there are several areas where all candidate countries should focus on: digitalization of the justice system, strengthening of digital infrastructure, economic policies oriented to clean and digital transitions, interoperability of technological assets such as the identity wallet (such as the Balkan Digital Identity Wallet or the WiFi4EU initiative in Western Balkans), the inclusion of the region in the European Digital Innovation Hubs, regional connectivity through digital infrastructure for transport and energy sectors, and agreements on electronic communications regulatory convergence, roaming agreements with telecom operators, convergence with the EU 5G Cybersecurity Toolbox, cyber resilience frameworks, the facilitation of the development of research infrastructures, science and technology parks, the promotion of technology transfer schemes, and innovation support measures.

Albania[xlviii] needs to address several areas to align with EU standards and improve digital integration. In **electronic communications**, the rollout of the 112 emergency number is incomplete, and fixed internet broadband access remains inequitable, especially in rural areas. **Digital services** require efforts to ensure equal access and alignment with the Digital Services and Digital Markets Acts. In **digital skills**, further progress is needed to expand ICT curricula and training programs. **Cybersecurity** demands greater focus on protecting critical infrastructure, operationalizing the new national security operations center, adopting the cybersecurity action plan, and enhancing cooperation with private sectors. Legislative updates are pending in **electronic identification** to align with the EU Digital Identity framework and for the **ePrivacy Directive**. The **700 MHz band** needs to be released for mobile communications, including 5G, to prevent interference with neighboring countries. Moreover, improvements in **statistical data collection** are required to meet the Digital Economy and Society Index standards. Finally, in **media**, the Audiovisual Media Authority (AMA) needs better resources to enhance monitoring and reporting capacity, with no significant legislative developments since the 2023 Broadcasting Code approval.

Bosnia and Herzegovina[xlix] faces significant challenges in aligning with EU standards across digital and media policy areas. The country lacks a broadband strategy, has not aligned electronic communications laws with the EU acquis, and faces delays in 5G licensing until at least 2026. The Communications Regulatory Agency suffers from political and financial dependency, with its board's mandate expired since 2017. Digital services lack a national strategy, open data policy, and coordinated transformation, requiring alignment with EU frameworks like the Digital Services Act. Cybersecurity is underdeveloped, with no national strategy, legislative framework, or operational cybersecurity infrastructure such as CSIRTs. Additionally, legislation on electronic identity and signature interoperability remains unaddressed. In media, despite progress in digital broadcasting, public broadcasters lack financial sustainability and political independence, necessitating reforms in fee collection and governance to comply with EU standards and reduce political influence.

Montenegro[l] has made progress in aligning with EU standards but still needs to address key policy areas. In **electronic communications**, while national legislation aligns with the European Electronics Communication Code, the government must adopt a National Plan for broadband infrastructure development and align with the Gigabit Infrastructure Act. In **cybersecurity**, Montenegro needs to establish a Cybersecurity Agency, meet critical infrastructure requirements, implement the 5G Cybersecurity Toolbox, and align with the e-Privacy Directive. Further efforts are required to align with the EU Digital Identity and Trust Services framework. In **digital services**, Montenegro should accelerate alignment with the Digital Services Act and Digital Markets Act to provide business predictability. Lastly, in the **media sector**, Montenegro must ensure the effective functioning of its restructured audiovisual regulator, AMU, strengthen its capacity to monitor the audiovisual market, and promote media literacy to solidify recent legislative advancements and cultural program participation.

North Macedonia[li] needs to address several policy gaps to advance its digital transformation and align with EU standards. The country has yet to adopt long-term ICT and national cybersecurity strategies, and the Ministry of Digital Transformation must strengthen its capacity to coordinate policies effectively. In **electronic communications**, alignment with the EU Broadband Cost Reduction Directive is pending, and the independence of the regulator remains a concern after the dismissal of the AEC Commission. Fixed broadband coverage is substantial, but the 112 emergency services require enhancement. **Digital services** need improvement, with many critical services like issuing personal documents unavailable online and incomplete upgrades to the national e-portal. Efforts to align with the Digital Services Act, Digital Markets Act, and European Interoperability Framework must be prioritized. In **cybersecurity**, adopting the NIS2-aligned Law on security of networks, bolstering the national cybersecurity center, and addressing the cost and usability of e-identification tools are essential. **Media sector** challenges include delays in appointing regulatory members, enhancing oversight of new media formats, and concerns over reintroduced government advertising in private media. Lastly, alignment with the ePrivacy Directive and further expansion of broadband access in underserved areas remain critical goals.

Georgia[lii] lacks an overarching digital strategy despite announcing priorities like artificial intelligence and agrotechnology. In **electronic communications**, while progress was made with adopting the e-commerce Law and Broadband Cost Reduction Directive by-laws, Georgia still needs to align with the European Electronic Communications Code, the Regulation on geo-blocking, and platform-to-business relations. The ongoing 5G rollout shows alignment with EU standards, but further development is required. **Digital services** need significant improvement, with partial alignment on open data reuse and limited progress on the Digital Services Act (DSA) and Digital Markets Act (DMA). Alignment with the GDPR, AI Act, and EU AI innovation best practices is also necessary. In **cybersecurity**, the national strategy would benefit from closer adherence to the NIS2 Directive, and a National Interoperability Framework aligned with the European Interoperability Framework is needed to enhance cross-border digital services. **Media regulation** has improved with amendments to the broadcasting law addressing the protection of minors and self-regulation, but the independence of the national media regulator requires safeguarding. Finally, Georgia has made progress in **media and information literacy** by integrating it into formal education, training teachers, and developing resources, but continued efforts are needed to enhance digital literacy broadly.

Moldova[liii] has made progress in digital transformation, establishing a National Council for Digital Transformation in 2023 to implement the 2023-2030 strategy. It has started aligning with the EU Roaming acquis and the European Electronic Communications Code, while the National Regulatory Agency (ANRCETI) has taken over civil radio frequency management. Moldova ratified the Digital Europe programme association in May 2024, opening opportunities for EU projects. However, alignment with the Digital Services Act (DSA), Digital Markets Act (DMA), and open data policies remains insufficient. On cybersecurity, the newly established Cybersecurity Agency needs further operational strengthening, and media regulation improvements are ongoing.

Serbia[liv] needs to ensure the full operational and financial independence of the Regulatory Agency for Electronic Communications (RATEL) and improve its administrative capacity. Although Serbia adopted a new electronic communications strategy in 2024, the broadband law and 5G frequency auction legislation are still pending. Serbia also needs to align with the Digital Services and Digital Markets Acts, the EU Open Data Directive, and the AI Act by 2025. In cybersecurity, further alignment with the NIS 2 Directive and the European Digital Identity framework is required. Media regulation improvements are ongoing, but concerns remain regarding independence, media pluralism, and full implementation of media laws.

In **Turkey**[lv]**,** although the e-commerce market has expanded, alignment with the Digital Services Act and Digital Markets Act is needed. Existing digital services legislation, such as the Social Media and Disinformation Laws, conflicts with EU principles on freedom of expression. Türkiye's e-government services have grown, but alignment with the European Interoperability Framework is required. Broadband competition remains weak, and progress on 5G procurement is slow. Türkiye must improve cybersecurity, continue implementing the 5G Cybersecurity Toolbox, and enhance media regulation clarity and independence.

Ukraine[lvi] has made progress in aligning its electronic communications and digital services with EU standards, including adopting legislation on EU roaming and working on the regulatory framework for radio spectrum policy, though security concerns delay the release of the 700 MHz band. It continues developing its e-government system, seeking alignment with the European Interoperability Framework and the Digital Services Act. Ukraine has made strides in digital trust and cybersecurity, aligning with the European Digital Identity Regulation and implementing a national cybersecurity strategy. In media, Ukraine's legislation aligns with the Audiovisual Media Services Directive, though restrictions on Russian TV channels remain due to security concerns.

While it is unknown whether or not, when and which countries will enter the European Union, the EU's enlargement policy will be a **central element in the coming years and digital policy is a significant element due to its impact on the security, resilience and economic competitiveness of the European Union**.

4.6 Strengthening the voice from Member States in the EU's Economic Security Strategy proposal and its related initiatives

The European Commission proposed in the summer of 2023 the first-of-its-kind Economic Security Strategy, which aims to address the economic security risks derived from certain economic flows and activities that may remain vulnerable or threatened in the current scenario of geopolitical tensions and accelerated technological development.

The European Economic Security Strategy is based on a three-pillar approach, or three Ps: **promotion** of the EU's economic base and competitiveness; **protection** against risks; and **partnership** with countries with shared concerns and interests. The four areas that require risk assessment are: resilience of supply chains, including energy security; physical and cyber-security of critical infrastructure; technology security and leakage; and weaponization of economic dependencies and coercion.

Concretely, one of the first deliverables has been the list proposal on critical technologies by the European Commission, which encourages Member States to provide their risk assessments and lead to a collective work to determine which proportionate and precise measures should be taken to promote, protect and partner in specific technological areas. The goal is two-fold: to reduce dependencies from third actors whose supply chain and political security may be of high-risk, and to promote a diversification of strategic assets across the Union and with trusted partners.

The proposal for a European Economic Security Strategy emphasizes **cooperation between the European Commission and EU Member States** to strengthen economic security across various dimensions. Key actions for Member States include developing a shared framework for assessing economic risks, particularly regarding critical technologies, and engaging in a structured dialogue with the private sector to enhance risk management. Member States are also encouraged to coordinate on foreign investment screening, address outbound investment risks, and improve research security across the EU. Additionally, national efforts are expected to align with EU initiatives on export controls, dual-use technologies, and cybersecurity tools.

For this to happen, Member States, including Greece, Italy, Portugal and Spain, need to reflect on their own national approaches on how to Promote innovation, Protect our competitiveness and our technological capabilities, and Partner with trusted partners outside the EU but also through a strengthening of the cooperation across Member States.

Cooperation and coordination with Member States is particularly important due to the overall negative situation of EU's leadership in **critical technologies**. According to DigitalEurope's Critical Technologies Gap report[lvii], the EU faces three major challenges in regaining its position as a global technology leader:

1. **Scalability Issues**: Fragmentation within the single market and the absence of a unified strategy limit EU companies' ability to grow and compete internationally.

2. **Investment Gaps**: Europe lags behind the US and China in investing in capital-intensive critical technologies, with fragmented public funding and inefficiencies in research commercialization.

3. **Regulatory Barriers**: Stringent EU regulations, unmatched elsewhere, create a competitive disadvantage for European companies, preventing them from growing and scaling within the region.

The EU is falling behind in critical technologies, with the US leading in most sectors, and China excelling in energy technologies. Despite strong R&D capabilities, the EU faces challenges in scaling, manufacturing, and commercializing innovations. A significant investment gap in AI, quantum computing, and space technologies hampers competitiveness. Additionally, complex regulations and restrictive funding hinder business growth, while a shortage of tech talent in key areas exacerbates the problem.

To remain competitive, the EU must strengthen global partnerships, enhance supply chain resilience, leverage its leadership in global standards, and establish priority-setting, timelines, expected outcomes and coordination mechanisms to reach its goals during the 2024-2029 period.

Concluding remarks and policy recommendations

The PromethEUs position paper of April 2024, “Digital for Growth: Strengthening the Single Market and Reviving EU Competitiveness,” provided **10 recommendations**. Based also on the elements and findings presented in this document, we elaborate on these in turn.

Regulation

1. **Reducing red tape at EU and national level, especially for startups and other entities expanding internationally**
   In the context of the Letta Report, which refers to a "European Code of Business Law" and the transformation of the Single Market into a "European Market" by providing businesses, especially SMEs and startups, a "28th regime to operate within the Single Market", it can be argued that the establishment of a clear, effective, and consolidated regulatory framework is key.
   On the one hand, this framework can reduce regulatory hold-ups through the implementation of regulatory and administrative fast-track mechanisms. On the other, it can establish a substantial regulatory one-stop-shop, which could be conceived as a EU portal where startups can access centralised information from across Member States and submit permit and licence requests that enable them to operate in multiple countries. Furthermore, we agree on the value of establishing regulatory sandboxes, which would enable startups to test new digital products and services, thereby reducing the risk and burden of regulatory compliance. For example, a suitable model can be found in the AI Act, since it allows for extensive collaboration both within a single MS and across MSs.
   As well, transparent procedures under the DMA need to be established to facilitate the submission and resolution of complaints from startups promptly and efficiently. Additionally, the revision of the GDPR’s procedural aspects presents a valuable opportunity to enhance the efficacy with which the functioning and mechanisms of complaints, as well as the role of complainants, are addressed.

2. **Streamlining EU digital legislation, making it simpler and increasing consistency**
   As previously stated, digital providers are currently facing the challenge of navigating the complex landscape of over 100 existing and forthcoming laws. This burden could be alleviated through the integration of a number of instruments, including the provision of consolidated legal texts, the compilation and reconciliation of existing legislation, and the elimination of redundancies and inconsistencies. This issue has been a central focus of Commissioner Virkkunen’s hearing, as well as of both the Draghi and Letta Reports. In particular, the former report suggests that the rules for transposing EU directives should be improved by establishing a uniform standard for all Member States and conducting a stress

test on the existing regulatory framework for at least six months at the outset of each Commission's term. The latter proposes that the current regulatory framework should first be codified, and that innovative measures and new EU instruments should then be introduced, tailored to the specific needs of businesses.

These recommendations are undoubtedly pragmatic in nature and are aimed at ensuring legal certainty and operational clarity for businesses. This is of particular importance for smaller enterprises, those with limited financial resources, and companies operating across multiple Member States. In order to ensure a coherent and effective legal framework for the remainder of the Digital Decade, it is essential to eliminate any overlaps between the various legal instruments currently in place. Alternatively, clear guidelines on the joint application of these instruments should be published. Furthermore, efforts should be made to simplify and unify compliance and reporting procedures across different legal instruments, as well as to streamline data privacy rules for companies with users in multiple countries.

Moreover, we advocate the implementation of "Better Regulation" principles in the creation, revision, and repeal of EU legal instruments, as emphasised in the Draghi Report. This approach is of vital importance in fostering a regulatory environment that is conducive to innovation, reduces administrative burdens, and enhances the competitiveness of European businesses.

3. **Facilitating interoperability and open digital ecosystems**

As highlighted in the Draghi Report, the European Commission should go beyond the remit of the DMA in advancing interoperability and fostering the creation of open digital ecosystems. The following key actions could be undertaken to achieve this: a) the completion of the EU data spaces (leveraging also their scale) would enable EU businesses of all sizes to tap into shared resources, driving innovation and enhancing competitiveness within the Single Market. This would also be supported by standardised procedures, effective data management/protection, and quality assurance mechanisms; b) the DMA and DSA should be enforced quickly and effectively to foster a fair, transparent, and open digital environment; c) the promotion of open common standards for service and data interoperability; d) the enactment of regulations mandating or incentivising the use of open Application Programming Interfaces (APIs), particularly in sectors such as healthcare, smart cities, or finance, where the benefits of interoperability can result in significant societal and economic outcomes; e) supporting open-source initiatives that promote interoperability, ensuring that innovative solutions become more accessible to a broader range of stakeholders, including SMEs and startups.

Investment

4. **Within the reassessment of EU budget priorities towards the next Multiannual financial framework, the budget of the Digital Europe program should be markedly revised upward**
   The lack of ambition for digital investment targets contrasts with the overarching goal of the EU Digital Programme to build a globally competitive digital ecosystem.
   Within the reassessment of EU budget priorities (e.g., the growing focus on defence and security), the budget of the Digital Europe Programme should be markedly revised upwards. As mentioned above, the current budget (less than €10 bn over 7 years in 5 technological fields) does not even match individual investments by the world's largest companies in one single technology.

5. **Introducing more coordination in key technology investment**
   The EU budget not only needs to be increased but also better coordinated with other EU programmes, and especially with Member States. For instance, the coordinated plan for AI, started in 2018, should be resumed and strengthened, as well as its governance. Some form of sanctioning mechanisms should be set in place for non-compliance.
   Moreover, IPCEIs and Joint Undertakings such as the EuroHPC should be strengthened and extended to other digital technologies, streamlining bureaucracy, speeding up processes and improving the access of SMEs to these initiatives.
   For R&D, lighthouse research centers should be set up at EU level for strategic technologies, open to public-private partnerships, coordinating networks including research and academic institutions from MSs and collaborating with non-EU entities.

6. **Accelerating the Capital Markets Union**
   Moreover, to ensure that European startups and companies grow and become key players in the digital market, it is essential to accelerate the European capital market, promoting greater integration and simplifying access to funds. Especially in the startup and scaleup phase, companies would benefit from better well-functioning European markets for risk capital. At present, foreign investments dominate the scaleup funding rounds. Dynamic and innovative EU businesses often do not have sufficient capital to compete globally and are obliged to seek funding abroad or to relocate overseas. European tech startups, for example, are much more frequently acquired by US firms than the other way round. This can be explained by the lack of access to venture capital (VC) investments compared to the US, where VC investments were ten times higher than in the EU in 2022.

Empowering SMEs

7. **Targeting SMEs with specific programs to upskill and reskill current management and workforce**
   The twin transitions of digitalization and sustainability present both formidable challenges and transformative opportunities for SMEs in Southern Europe. These enterprises, which form the backbone of regional economies, must adapt to remain competitive in a globalized market increasingly driven by technological advancements and green imperatives. Upskilling and reskilling programs are vital in equipping SME workforces with the necessary capabilities to navigate this changing landscape. These programs not only address skill gaps but also enhance innovation, inclusiveness, and economic resilience, enabling SMEs to thrive amidst shifting market dynamics.

8. **Speeding up the creation of sectoral dataspaces**
   Equally transformative are sectoral dataspaces, which provide the digital infrastructure for secure and transparent data sharing. By fostering collaboration within and across industries, dataspaces empower SMEs to leverage data-driven solutions to optimize operations, enhance sustainability, and drive competitiveness. Relevant initiatives -such as Spain's leadership in the European Mobility Data Space and Greece's focus on smart agriculture- are enabling SMEs to modernize traditional industries and seize new growth opportunities. Portugal's and Italy's strategic emphasis on energy and manufacturing dataspaces further underscores the importance of aligning national priorities with the EU's broader vision for a sustainable and digitally integrated economy.
   Despite these advancements, challenges persist, including disparities in digital infrastructure, regulatory complexities, financial barriers, and cultural resistance to innovation. Addressing these obstacles requires a multi-faceted approach, combining investments in infrastructure, regulatory harmonization, and targeted training programs. The role of collaborative ecosystems, including Digital Innovation Hubs and the Enterprise Europe Network, is crucial in bridging resource gaps and fostering knowledge exchange.

.

Geopolitics

9. **Encouraging and entrusting digital diplomacy**
   The new Commissioner-designate for Tech Sovereignty, Security, and Democracy should prioritize digital diplomacy, focusing on strengthening EU competitiveness in critical technologies like quantum computing and semiconductors. The EU's strategy should include leveraging partnerships with global leaders like Japan, South Korea, and the US, as well as fostering innovation through Horizon Europe and the Chips Joint Undertaking. Key areas of focus should be AI development, strengthening supply chains, and engaging in international governance efforts like the UN-led Global Digital Compact. EU Member States should play a

critical role in ensuring coherence, facilitating joint investments, and contributing to global digital standard-setting initiatives.

Also, the EU should prioritize becoming a global leader in digital diplomacy by promoting human rights, strengthening digital sovereignty, and enhancing geopolitical influence. It should integrate digital diplomacy into existing policies and foster international collaborations to influence global technology standards. To counter cyber threats, the EU should strengthen digital security mechanisms and invest in partnerships. Additionally, it should focus on building capacity, enhancing diplomats' expertise, and establishing regional digital diplomacy hubs. The EU must also ensure effective monitoring of technological developments and align digital policies with democratic values and human rights.

The EU should prioritize digital diplomacy with candidate countries for accession, including Ukraine, Georgia, Moldova, and others. Key areas of focus include aligning digital policies on telecommunications, cybersecurity, data protection, and technical standards. These countries also face external challenges, such as disinformation and vulnerabilities in critical infrastructure. EU engagement should help overcome these issues, ensuring resilience against harmful influences. Candidate countries should enhance digital infrastructures, improve digital justice systems, and integrate into EU initiatives like the European Digital Innovation Hubs, aiming for greater economic and technological alignment with the EU. Digital policy is critical for future EU enlargement.

10. Using public procurement to increase demand for innovation

National public procurement framework conditions should be more conducive to innovation. The European Commission has taken significant action to promote Public Procurement for Innovation (PPI) through policy formulation, funding programmes and regulation directives. Member States should further adapt these directives to their national legislation in order to create an innovation-friendly public procurement framework not characterized by mere cost effectiveness rationalization. For instance, national regulations should provide room for the development of innovative and out-of-the-box solutions by favouring the use of functional based requirements in tendering processes and by promoting the creative interaction between demand and supply. Pre-commercial public procurement (PCP) is also an approach that may address shortcomings such as lack of active dialogue between the public buyers and potential suppliers, and risk aversion on both the public and private sides.

Furthermore, framework conditions should aim to achieve a balance in the participation of experienced large firms and specialized smaller providers in innovative procurement practices. Therefore, national regulations should facilitate the access of SMEs to public procurement by providing the opportunity for splitting tenders into lots, encouraging SMEs to bid jointly, reserving a share of the total procurement budget for contracts or direct grants to small/micro-firms as well as simplifying and digitizing the tender procedures.

Furthermore, policy measures should develop and strengthen specific skills and organizational capabilities to successfully design and manage such procurement practices. Such measures should focus on strengthening the public procuring agencies' staff in terms of technical, managerial and legal skills and competencies to support the design and implementation of PPI practices. They could include training schemes, guide tools and learning mechanisms such as best practice networks and peer-to-peer training of public procurement professionals. In addition, financial support could be provided to public buyers in order to acquire high-level staff and/or external expertise consultancy.

Finally, a critical capability for the successful realization of complex eGovernment projects is the extensive collaboration and interaction between the public procurer and the supply-side entities during all phases of the procurement process, i.e. from idea generation to full-scale delivery and operation of the procured system. Such a capability can significantly contribute to the clear translation of the procurer needs into specific functional requirements, the efficient management of technological and market risks (i.e. the selection of appropriate suppliers), and ultimately the effective coordination, implementation and beneficial completion of complex projects.

References

[i] https://eur-lex.europa.eu/eli/dec/2022/2481/oj
[ii] ZENNER J., MARCUS J. S., SEKUT K. (2024), A dataset on EU legislation for the digital world (www.bruegel.org)
[iii] https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-ai-act-prohibitions-and-ai-system-definition
[iv]https://digital-strategy.ec.europa.eu/en/library/first-draft-general-purpose-ai-code-practice-published-written-independent-experts
[v] https://digital-strategy.ec.europa.eu/en/policies/ai-pact
[vi] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en
[vii] German Council on Foreign Relations, *Europe's Capacity to Act in the Global Tech Race. Charting a Path for Europe in Times of Major Technological Disruption*, 2021
[viii] *Report, THE FUTURE OF EUROPEAN COMPETITIVENESS — PART B, 2024*
[ix] https://digital-strategy.ec.europa.eu/en/activities/funding-digital
[x] German Council on Foreign Relations, *Europe's Capacity to Act in the Global Tech Race. Charting a Path for Europe in Times of Major Technological Disruption*, 2021
[xi] Stanford University, AI Index Report, 2024
[xii] *Report, THE FUTURE OF EUROPEAN COMPETITIVENESS — PART B, 2024*
[xiii] https://www.top500.org/lists/top500/2024/06/
[xiv] https://digital-strategy.ec.europa.eu/en/factpages/quantum-and-supercomputing
[xv] https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship
[xvi] https://digital-strategy.ec.europa.eu/en/policies/quantum
[xvii] https://digital-strategy.ec.europa.eu/en/library/european-declaration-quantum-technologies
[xviii] *Report, THE FUTURE OF EUROPEAN COMPETITIVENESS — PART B, 2024*
[xix] https://worldpopulationreview.com/country-rankings/semiconductor-manufacturing-by-country
[xx] https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en
[xxi] https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade
[xxii] https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/sme-strategy-sustainable-and-digital-europe
[xxiii] https://een.ec.europa.eu/
[xxiv] https://digital-strategy.ec.europa.eu/en/activities/edihs
[xxv] https://ec.europa.eu/growth/smes/cosme_en
[xxvi] https://reskilling4employment.eu/es/espana/
[xxvii] https://digital-skills-jobs.europa.eu/en/opportunities/training/dis4sme-training-courses-smes
[xxviii] https://reskilling4employment.eu/en/portugal/
[xxix] https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/sme-strategy-sustainable-and-digital-europe
[xxx] https://www.cedefop.europa.eu/en/news/italy-national-strategic-plan-upskilling-and-reskilling-adults
[xxxi] https://pact-for-skills.ec.europa.eu/index_en
[xxxii] https://ec.europa.eu/newsroom/empl/items/848844/
[xxxiii] https://digital-strategy.ec.europa.eu/en/policies/strategy-data
[xxxiv] https://gaia-x.eu/
[xxxv] https://datos.gob.es/sites/default/files/blog/file/infografia-gaia-datos-europeos_en_0.pdf
[xxxvi] https://data.europa.eu/sites/default/files/course/Slides_EMDS_webinar.pdf
[xxxvii] https://datos.gob.es/en/blog/national-health-data-space-strategic-project-country
[xxxviii] https://internationaldataspaces.org/make/network/
[xxxix] https://tice.pt/en/gaia-x
[xl] https://eithealth.eu/wp-content/uploads/2024/06/EHDS-white-paper-Portugal.pdf

[xli] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Transport-data-creating-a-common-European-mobility-data-space-communication-_en

[xlii] https://gaiax.gr/

[xliii] https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

[xliv] https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

[xlv] https://commission.europa.eu/document/3b537594-9264-4249-a912-5b102b7b49a3_en

[xlvi] https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/eu-digital-diplomacy-council-agrees-a-more-concerted-european-approach-to-the-challenges-posed-by-new-digital-technologies/

[xlvii] https://neighbourhood-enlargement.ec.europa.eu/document/download/7c67aed6-e7c2-47de-b3f8-b3edd26a3e26_en?filename=COM_2024_690_1_EN_ACT_part1_v11.pdf

[xlviii] https://neighbourhood-enlargement.ec.europa.eu/document/download/a8eec3f9-b2ec-4cb1-8748-9058854dbc68_en?filename=Albania%20Report%202024.pdf

[xlix] https://neighbourhood-enlargement.ec.europa.eu/document/download/451db011-6779-40ea-b34b-a0eeda451746_en?filename=Bosnia%20and%20Herzegovina%20Report%202024.pdf

[l] https://neighbourhood-enlargement.ec.europa.eu/document/download/a41cf419-5473-4659-a3f3-af4bc8ed243b_en?filename=Montenegro%20Report%202024.pdf

[li] https://neighbourhood-enlargement.ec.europa.eu/document/download/5f0c9185-ce46-46fc-bf44-82318ab47e88_en?filename=North%20Macedonia%20Report%202024.pdf

[lii] https://neighbourhood-enlargement.ec.europa.eu/document/download/7b6ed47c-ecde-41a2-99ea-41683dc2d1bd_en?filename=Georgia%20Report%202024.pdf

[liii] https://neighbourhood-enlargement.ec.europa.eu/document/download/858717b3-f8ef-4514-89fe-54a6aa15ef69_en?filename=Moldova%20Report%202024.pdf

[liv] https://neighbourhood-enlargement.ec.europa.eu/document/download/3c8c2d7f-bff7-44eb-b868-414730cc5902_en?filename=Serbia%20Report%202024.pdf

[lv] https://neighbourhood-enlargement.ec.europa.eu/document/download/8010c4db-6ef8-4c85-aa06-814408921c89_en?filename=T%C3%BCrkiye%20Report%202024.pdf

[lvi] https://neighbourhood-enlargement.ec.europa.eu/document/download/1924a044-b30f-48a2-99c1-50edeac14da1_en?filename=Ukraine%20Report%202024.pdf

[lvii] https://www.digitaleurope.org/resources/the-eus-critical-tech-gap-rethinking-economic-security-to-put-europe-back-on-the-map/