

PromethEUs Joint Paper

The Multisided Path to European Digital Sovereignty and the future of EU-US Relations

Executive summary

This paper explores the concept of **digital sovereignty** applied to the European Union, placing the current policy initiatives, regulatory interventions and international relations, especially with the US, in this context. **It is the result of the collaboration of four think tanks from Southern Europe (Greece, Italy, Portugal and Spain), sharing some common problems and challenges.**

The topic is gaining particular prominence since digital markets and technology are now dominant in every aspect of societies and economies around the globe. Due to their prominence, strategic autonomy concerning technological and digital assets is at the top of the European economic, social and geopolitical agenda. However, there are different possible declinations of the concrete meaning of digital sovereignty. **This paper clearly rejects protectionist stances, opportunistically derived from an extreme notion of sovereignty, while embracing the aspiration to play a greater role independently exercised by Europe on the global stage, open to a fruitful collaboration with other world areas and countries, starting with our main ally, the US.** To achieve this, a fundamental contribution needs to come from the quantity and quality of technological investments, a set of rules able to protect consumers and citizens without stifling innovation and the development of new diplomatic fora such as the EU-US Trade and Technology Council, alongside the existing ones.

Chapter 1 points out that the discussion around digital sovereignty is a part of a broader effort by the EU to reinforce the Union's general strategic autonomy in areas ranging from energy to health. **Digital sovereignty is especially important in the EU, due to the clear competitive disadvantage that the Member States (MSs) currently have compared to the US and China.** Because of this disadvantage, the EU has become increasingly dependent on foreign suppliers, such as technology companies from the US, China, and Taiwan, to obtain strategic technology.

To reduce this competitive gap, the EU has launched several investment initiatives such as GAIA X (EU sovereign cloud), 5G PPP, and Horizon 2020. Such initiatives are to ensure that the EU strengthens its ability for autonomous action in the digital field. They also aim at assuring that the Union holds the tools to ensure that EU citizens' rights and freedoms are protected.

Apart from the economic aspects of the digital realm, there are also substantial differences in how the EU conceives digital spaces when compared with the US and China. The EU envisages a secure

and fair digital environment that may allow citizens to access digital hardware and software while guaranteeing that their rights are duly respected. To implement such a vision, the EU has put forward several regulatory initiatives (GDPR, DGA, DSA, DMA, NIS II Directive) addressing issues that range from consumer protection to cybersecurity regulations.

Chapter 2 recalls the reasons behind the **failure of the Lisbon Agenda of 2000**, when the EU aimed to become, in 10 years, “the most competitive and advanced knowledge economy in the world”. However, **Europe still lacks today enough private and public entrepreneurial élan, a large enough venture capital market, and sufficient advanced technological and digital skills among its population and its professionals.** In the 1990s, the EU was a digital power, but it has lost ground and increased its digital dependence on foreign companies (American, but also Chinese and from other countries).

The search for a European digital sovereignty, or autonomy, has led the EU and its MSs to dedicate more brain power and more financial resources to achieve this aim, with a flurry of proposals from the European Commission, the European Parliament and the MSs. The Commission has presented a promising system of governance that merits support for technological itineraries for the EU and its MSs, and for a proposal where Brussels (Council, Commission and Parliament) would monitor the progress of each MS towards the goals of the digital decade. This goes well beyond the OMC of 20 years ago. Each country would draw up an itinerary, a National Digital Decade Strategic Roadmap. The proposed decision sets **digital targets for 2030 based on “four cardinal points” - digital skills, digital infrastructures, digitalisation of businesses and of public services.** It would be a kind of “European Digital Semester”, along the lines of the “European Semester for the Economy”. The starting point is the need for common governance and coordinated investments, but excluding new common resources following the efforts of the NextGeneration Fund.

Chapter 3 focuses on how, based on the scenario of EU’s growing over-dependence on foreign-owned technology providers, it is strongly working to harness public-led initiatives to foster the private sector. Concretely, the EU is doing so by supporting technology areas. The area most restraining Europe’s capacity to act in the global tech race with its own European companies, and the one where the EU has the highest level of dependence on non-EU countries, is **cloud computing.** Thus, it is not by chance that cloud computing has been the technology area where the EU, and overall its MSs, have worked the most on supporting European projects and European firms through governmental coordination, funding, or resource pooling.

In the quest to safeguard Europe’s global technological sovereignty, previous attempts to foster cloud computing providers in Europe have resulted in important policy lessons for the current proposals of GAIA-X, the IPCEI-CIS on cloud infrastructure, and the European Alliance on Data, Edge and Cloud. The cases of the French government-led Andròmede sovereign cloud project in 2009, the German De-Mail project as a secure tool for communications, and the Franco-German Quaero initiative have highlighted specific policy issues on communication, institutional learning

and coordination and bureaucratic issues, going well beyond the technical dimension of the issue. This part of the chapter provides policy recommendations, looking back at mistakes and strengths from the past, and seeking to strengthen current attempts, namely GAIA-X, IPCEI-CIS and the European Alliance, to move European technology power forward.

Chapter 4 measures the level of digitalisation of the EU MSs, compared with other advanced countries. In the *I-DESI 2020*, compiled by the European Commission, the US score is the highest, while the top four countries of the EU rank second, followed by Switzerland, Norway and Iceland. However, **the EU average is below the main digital countries such as Korea and Japan. A critical issue that should be considered is the considerable disparities among the EU states since the EU bottom four countries rank 15th in the I-DESI, after Russia.** The average performance of the EU bottom four countries appears almost in the ranking's last positions for most of the I-DESI sub-dimensions. In contrast, the EU top four countries rank in the first three positions in most of them. Similar results are provided for the rest of the indicators examined.

European companies are less developed in the spread of digital technologies and the use of those technologies for new services and business models. Therefore, the rapid growth of non-EU technology firms could significantly constrain the development of EU high-technology companies and the ability of policy-making at the EU level. According to the European Investment Bank Survey (EIBIS) in 2020, the performance of the US is much more prominent. However, differences among EU countries are apparent, with adoption rates ranging from 47% to 76%. **In most of the examined digital indicators, a critical gap between Northern and Southern Europe is observed.**

A key component for successful digital transformation is the adoption and development of AI technologies. Regarding research peer-reviewed AI publications in 2019, China held the lion's share, followed by the EU and the US. Historically, the EU was the leader in terms of AI scientific publications, however, it appears that China made a critical leap in the last year, and the EU should now focus on regaining its leading position. As well, in hybrid academic-corporate publications, the EU is behind, while the US is leading in the field. Therefore, Europe needs to focus on regaining its leading position in AI research and, at the same time, to create an encouraging policy framework for corporate-academic synergies and the commercialisation of the produced research. Otherwise, there is a great risk for the EU to miss the opportunity to establish its sovereignty.

The US is leading worldwide in patent applications, and China is more prominent in data collection and data access, the primary source for developing AI technologies. Start-up firms established in the US and China in the VC share absorbed more than 80% of investments in 2020. The EU was next with only 4%, and the UK and Israel, both at 3%. Within the EU, AI firms in Germany and France absorbed two-thirds of VC investments in 2020.

After the pandemic outbreak, a unique opportunity was created for more traditional sectors to digitalise their business models for their competitiveness and, generally, economic growth. **To explore further the determinants of digital integration by firms, we conducted a short exercise by utilising the data of the I-DESI for the period 2015-2018.** Our objective is to stress the key factors

that enable firms to optimise their technological integration fully. Our analysis does not intend to establish causality but only to find significant correlations among the different dimensions of digital advancement. **Our results indicate that if a government aims to increase its integration of technology, the most critical factors in climbing the I-DESI ranking, *ceteris paribus*, are the dimension of citizen use of the Internet in general, and when considering sub-dimensions: a) fixed broadband take-up; b) mobile broadband take-up; c) at least basic skills (word processing); d) at least basic software (coding); and e) fixed broadband traffic (GB/mth/person).**

Chapter 5 discusses the evolution of the digital regulatory framework in the EU and US and presents the major milestones in recent decades. First, an historical description and assessment are conducted over the evolution of the EU digital strategy in the last 20 years. **The analysis focuses on the major milestones in three pillars - data, AI and online platforms and intermediaries.**

In the first section, the chapter recalls: the commitment to set up the European federal cloud within the framework of the Gaia X project; the **GDPR**, the well-known regulation approved in 2016 that provides a very strict framework for privacy and data protection; the joint declaration promoting the creation of an EU Cloud Rulebook; and the European Alliance for Industrial Data and the Cloud, created in December 2020. Moreover, the **Communication “A European strategy for data”**, published by the Commission in February 2020, and then a proposal for a regulation on European data governance (**Data Governance Act**) published in November 2020 are presented and analysed. Where the second focus topic of AI is concerned, the EU began its pro-active approach on 25 April 2018, when the European Commission presented the Communication “AI for Europe”. Many initiatives have been undertaken since – including the publication, in February 2020, of the White Paper “Artificial Intelligence: a European Approach to excellence and trust”, and up to the launch of the AI Package in April 2021. This package includes a Communication on Fostering a European Approach to Artificial Intelligence, the Coordinated Plan with MSs: 2021, an update and a proposal for an AI Regulation laying down harmonised rules for the EU (**Artificial Intelligence Act**).

Following, given the increasing role played by platforms (especially by large ones), a specific analysis on the evolution of the regulatory framework in this field is conducted. The European Commission decided to revise the regulatory framework by introducing new responsibilities and obligations for platforms. To this end, on 15 December 2020, the European Commission published a package of two legislative initiatives - the **Digital Services Act (DSA)** and the **Digital Markets Act (DMA)**. After briefly recalling the previous regulations at EU level, the core elements and critical aspects of these two proposals are presented and discussed critically. **To conclude this first part, some potential limits and drawbacks of the EU regulatory approach, possibly achieving unintended consequences, stifling innovation and, at the same time, competition, are discussed.**

The second part of this chapter focuses on the US regulatory perspective, strongly conditioned by the overall vision of an essentially self-regulating market. A specific analysis of the major milestones in two key areas for the US system is presented - net neutrality and digital platforms.

The chapter also presents the US regulatory framework for digital platforms and focuses on three major aspects - **civil liability, freedom of speech and market power**. Finally, it looks at the role of large digital platforms, which have drawn the increasing attention of US antitrust organizations. Proof of this heightened interest is that, in February 2019, the Federal Trade Commission announced the launch of a task force to monitor technology-related markets, including online platform markets. Moreover, in 2021, several bills directed at large platforms and intermediaries were presented, both in the Senate and the House of Representatives, and from representatives of the two main political parties.

Chapter 6 affirms that, although the idea of a digitally autonomous EU may be attractive, to reach the forefront of technological development, the EU will need to ensure strong political and trading partnerships. Despite their differences, the EU and the US have the most important trade relationship in the world. In 2019, the US was the largest supplier of technological products to the EU and the biggest importer of those same goods and services from the EU. The recently inaugurated **Trade and Technology Council (TTC)** promises greater alignment between the EU and the US on topics related to digital strategic autonomy and reopens the discussion on sensitive topics such as the regulation of “big tech” companies. The TTC intends to restore transatlantic dialogue after several setbacks during the Trump administration. Its activity will focus on finding consensual solutions to address key economic challenges in several strategic sectors. **The Council is a promising platform to deepen transatlantic commercial ties, based on liberal democratic values and respect for human rights.** Areas of convergence include fostering investment in strategic technological assets, strengthening cybersecurity and cyber defence. **However, the TTC does not come without challenges.** While the EU sees regulation as a crucial tool for implementing a human-centred digital space, the US views EU regulation on digital markets and services as protectionist towards American businesses. **Apart from digital platform regulations, digital taxation, data protection, transfer and storage regulations may also give rise to controversy in the TTC’s discussions.**

CONTRIBUTORS

Chapter 1, Chapter 6 – IPP, Institute of Public Policy

Paulo Trigo Cortez Pereira

Steffen Hoernig

Tomás Le Terrien Fragoso

Chapter 2, Chapter 3 – Elcano Royal Institute

Andrés Ortega

Raquel Jorge Ricard

Chapter 4 – IOBE, Foundation for Economics & Industrial Research

Aggelos Tsakanikas

Maria-Theano Tagaraki

Chapter 5 – I-Com, Institute for Competitiveness

Stefano da Empoli

Silvia Compagnucci

Afroditi Karidomatis

Table of content

1. Digital Sovereignty: Concept and Context	10
1.1 Concept: Defining Digital Sovereignty	10
1.2 Main Features of Digital Sovereignty.....	11
1.2.1 Autonomy in crucial digital infrastructure and supply chains	11
1.2.2 Regulation of the digital economic landscape and legal autonomy.....	12
1.2.3 Control over citizen, business and governmental data	13
1.2.4 Tackling misinformation and improving cybersecurity	14
1.3 Context: why is digital sovereignty especially relevant in Europe?.....	15
1.3.1 Digital Sovereignty within the broader context of reinforcing EU strategic autonomy...15	
1.3.2 Mapping the EU’s competitive disadvantage in the digital realm.....	15
2. From the failed Lisbon Agenda to a European digital semester.....	17
2.1 The 1990s	17
2.2 Flaws in the Lisbon Strategy.....	18
2.3 The US, more of an entrepreneurial state and society than the EU	19
2.4 R&D, from lab to market.....	20
2.5 The insufficient European venture capital market	21
2.6 Management of skills, skilling and reskilling.....	22
2.7 European renewal?	23
2.8 From the OMC to the Monitoring and Cooperation Mechanism.....	25
3. Harnessing European Public-led initiatives with the private sector.....	27
3.1 European Union’s external dependence and the scenario of European technology companies	27
3.2 Cloud computing as the leading example of public support for private firms: the quest to leverage Europe’s global capacity to act in the tech race	28
3.2.1 Lessons from the past: “sovereign” cloud computing projects in Europe	29
3.3 Current attempts to revamp European technology sovereignty through public-led initiatives on cloud computing	32
3.3.1 EU Member State perspectives on cloud computing	32
3.3.2 Policy responses at the EU level	33
3.4 Policy opportunities to move European public-led initiatives forward.....	35

4. Convergence or divergence? Current digital trends in the EU, US and Asia	37
4.1 Current digital trends in the EU, US and Asia	37
4.1.1 National digital performance of the EU, US and Asia	37
4.1.2 Corporate digital performance of the EU, US and Asia	42
4.1.3 AI trends in the EU, US and Asia	44
4.2 Determinants of technology integration by firms at country level	46
4.2.1 Introduction	46
4.2.2 Results	47
5. Regulating the digital economy. A transatlantic perspective	49
5.1 The European Regulatory Framework	49
5.1.1 Digital sovereignty and the evolution of the European digital strategy.....	49
5.1.2 Data regulation: from the GDPR to the Data Act.....	51
5.1.3 The EU legal framework on Artificial Intelligence: from the Communication “AI for Europe” to the AI Act proposal	54
5.1.4 Platforms’ role and responsibility: from Directive 2000/31/CE to the DSA and DMA proposals.....	56
5.1.5 Limits and potential drawbacks of the EU regulatory approach	62
5.2 The Regulatory Framework in the US	64
5.2.1 The US approach to regulating the digital field	64
5.2.2 Net Neutrality in the US.....	65
5.2.3 Digital platform regulation in the US system.....	67
6. Resetting EU-US relations: common ground and challenges	71
6.1 The EU’s perspective on digital spaces and markets	71
6.1.1 European digital transition: investments and projects to close the gap between the EU and its competitors	71
6.1.2 The EU’s view on a fair and safe digital landscape	72
6.2 The Trade and Technology Council (TTC).....	73
6.2.1 Background and relevance.....	73
6.2.2 Structure and priorities	74
6.2.3 Challenges	76
6.2.4 Expected developments in the near future	78

Conclusions	80
Bibliography	85
Appendix	88
Data and Methodology	88

1. Digital Sovereignty: Concept and Context

1.1 Concept: Defining Digital Sovereignty

Digital technology has become an essential part of states, businesses, and people's daily lives. The digitalisation of companies is crucial to ensure their competitiveness. States rely on technology for managing most of their activities, as well as vital infrastructures such as dams, traffic lights, or railways. With the spread of smartphones, the Internet in general and the social media, citizens are also widely reliant on digital technology and platforms for professional and personal purposes.

The relevance of digital technology has brought it to the centre of political and geopolitical concerns, as renewed threats arise from the far-reaching pervasiveness of digital products and platforms. **Although the EU, the US and Japan dominated technology markets in the 1990s, the development of new technological powerhouses such as China and India raises renewed questions about the importance of controlling strategic digital technologies.**

The emergence of these new technological powers is leading to increased competition between those and previously dominant players, such as the US or the EU. The EU has now fallen behind some of the new players and become increasingly dependent on third-country technology.

The EU's technological dependence on both the US and China has raised strong concerns among MS leaders, on the Union's ability to protect its founding values and its citizens' rights from questionable practices such as surveillance and misuse of data by third countries. **It is against this background that the concept of digital sovereignty (or "technological sovereignty") is now at the centre of discussions in the EU.**

Digital sovereignty is the ability of states to act autonomously in the digital realm. It is a broad concept, which includes privacy, competition policy, infrastructure and geopolitical concerns. **It especially refers to the ability to regulate digital markets and platforms according to a set of fundamental values and the power to enforce this regulation with non-compliant actors.**

Control over digital technologies has become essential to maintain the EU's credibility, both internally and externally. Cyberattacks on governments and companies' intellectual property, and concerns about the use of citizens' data for business or political purposes, have become more common and may lead citizens to question the credibility of their respective governments to protect them from those threats. Hence, the increasing importance of digital sovereignty.

1.2 Main Features of Digital Sovereignty

In broad terms, digital sovereignty may refer to the ability of states to have control or act autonomously concerning: (i) crucial digital infrastructure and supply chains; (ii) the digital economic landscape; (iii) citizens' and governmental data; as well as (iv) cybersecurity and misinformation.

In the next sub-sections, we will provide an overview of each of these elements, with the objective of providing a deeper understanding of the relevance of digital sovereignty for societies' stability and progress.

1.2.1 Autonomy in crucial digital infrastructure and supply chains

One of the most important dimensions of digital sovereignty is a state's ability to control crucial digital infrastructure and supply chains. Without the control of these, economies will be dependent on the will of third countries and companies to supply raw materials or crucial technology.

Data storage is essential to making sure that citizens' sensitive information, such as health data, is correctly stored, and that data subjects can know in real time how their data is used. **States should ensure that cloud service providers store and treat data in line with citizens' privacy rights.** Storage facilities, such as **data centres, are essential infrastructures** to ensure that governments have the necessary alternatives, in case all available market alternatives fail to protect the data stored according to EU rules. **Investment in this type of physical infrastructure, as well as "sovereign clouds", may be determinant to ensure protection of data from undue access and usage.**

The EU is also dependent on the external supply of raw materials and other components, especially semiconductors, which are a key component for most electronic and many other devices. The importance of guaranteeing semiconductor supply chain resilience was proven during the Covid pandemic, when US and EU car factories had to stop production for lack of these microchips. Apart from semiconductors, other raw materials such as lithium or copper are also crucial for the production of digital devices.

Finally, the supply of crucial infrastructure by foreign players may also be risky, especially if those players do not share the same values as the EU. A good example of crucial infrastructure that is considered to entail risks is the use of 5G equipment by Huawei. Huawei 5G equipment was banned by the US on suspicion of connections to and effective control by the Chinese government. Although, the EU did not issue a formal ban on Huawei, it has identified the interference by third parties as one of the main security risks in implementing 5G in Europe¹.

¹ [EU countries keep different approaches to Huawei on 5G rollout – EURACTIV.com](#)

1.2.2 Regulation of the digital economic landscape and legal autonomy

The expansion of the digital sector has created new business models and realities. The emergence of digital markets has led to the need to adopt competition policy to cope with the special features of digital markets and spaces.

The ability of states to create legal frameworks to ensure fair competition within their national and regional markets is an important part of digital sovereignty. Ensuring fair competition in digital markets and the absence of abuses of market power are essential to foster innovation and reduce the effects of dependency on non-EU players.

Business models based on data extraction, transformation and selling of insights often lead to competition issues, as they tend to reward those companies with the largest market share. In addition to dominating data and advertising markets, influential digital players often acquire smaller companies when these may become potential competitors.²

To ensure fairness in digital markets, a robust framework of anti-trust regulation is essential. Such a framework must include measures to limit anti-competitive behaviour towards clients and competitors in the EU. The proposed Digital Markets Act of 2020 contains such a framework.

Many different aspects of the EU's digital economy that are not directly related to the power of gatekeepers, but that affect the rights and obligations of businesses and their customers, also need to be shaped by new rules, such as those foreseen in the Digital Service Act also proposed in 2020. Apart from putting into place legal frameworks that favour healthy competition and regulate digital activity, states must have adequate mechanisms to ensure that all players, including the most dominant, comply with such regulations.

MSs should also put forward robust legislation to filter misinformation and violent content, which threaten the very core of liberal democracies and have proven to boost political polarisation.

The ability to enforce these regulations is perhaps one of the most relevant aspects of digital sovereignty, as it translates into the sovereign power of states to decide the limits of private entities that provide their services in the EU and profit from the activity of its citizens in the digital realm.

Failing to protect EU citizens and businesses from abuse of market power or interference by foreign states puts both the internal and external credibility of MSs at stake.

² According to a report from the OECD ([oecd.org](https://www.oecd.org)), Amazon, Apple, Facebook, and Microsoft acquired 400 companies globally in the last 10 years (this number has increased to around 600 according to the Washington Post). [Amazon, Apple, Facebook, and Google became big tech companies by acquiring hundreds of smaller companies - Washington Post](#). According to the OECD, the four companies spent a total of US\$31.6 billion on acquiring start-ups."

Another dimension of digital markets that requires updated regulation is the ability to ensure that revenues generated by digital businesses are subject to tax in the EU, making sure that digital businesses pay their fair share on the income generated from their activity in any given MS.

1.2.3 Control over citizen, business and governmental data

Data is the fuel of the digital economy. The extraction of data in all fields, from human experience to natural events, is essential for business models whose activity is based on the provision of insights for targeted advertising. These insights, also known as behavioural futures, are valuable assets whose precision is dependent on the amount of data collected.

Concentration of data in the hands of a limited number of companies may undermine competition in data markets, and players that control more data (without sharing with other players) have more market power and incentives to abuse it.

Apart from the commercial usage of data, data may also be exploited for political purposes. The Cambridge Analytica scandal is the perfect example of how data from social media can be used to influence entire populations of voters with a specific political objective (Cambridge Analytica was a company specialised in political insights that used data from millions of social media users to profile entire populations to predict and influence voters' choices in the U.S. elections and the Brexit vote of 2016.). Misinformation campaigns by foreign actors, especially Russia, have been detected in a series of recent European election races.

Digital surveillance by non-EU states is a threat to EU countries' digital sovereignty. The US and India have banned TikTok under suspicion that its parent company - Byte Dance Ltd. – is sharing user data with the Chinese government under its National Security Law. The ban was reversed by the Biden administration, but suspicions remain that Byte Dance and other Chinese companies are sharing data with the Chinese central government.

The same types of concerns were recently raised concerning the 2018 US CLOUD Act. The act granted US law enforcement agencies the power to access foreign personal data stored in clouds provided by US service providers.

Finally, and no less important, is the control of crucial data by EU governments. A good example of how data usage by states is restricted by private players is the recent clash between the French and British authorities with Apple and Google over Covid-19 tracing apps. Apple and Google were accused of limiting EU sovereign power by refusing officials' requests to surrender user location data for Covid-19 tracing purposes, leaving the apps developed in the EU inoperable. As an alternative, some health authorities tried to set-up their own apps. However, the development of apps outside the Apple/Google ecosystems gave rise to other grave functionality issues.

These and other examples related to the use of data demonstrate that digital sovereignty is not reachable without “data sovereignty”: control over how citizens’ and essential governmental data is used and who has access to it. However, such control must be performed with caution and under a strict regulatory framework. Otherwise, governments may end up with excessive powers that may restrict the potential of digital economies and facilitate mass surveillance of civilians.

1.2.4 Tackling misinformation and improving cybersecurity

Cybercrime is expected to reach a cost of \$10.5 billion worldwide by 2025. Apart from the economic impact, societies’ security and stability are also at stake. The widespread digitalisation of services ranging from banking to health presents new opportunities for cyberattacks. Examples of such attacks are the 2017 attack on the UK’s NHS, which affected hospitals for several days, or the Russian hacking group ATP28’s attack on German government networks³.

Attacks may be performed for all sorts of reasons. Corporate espionage, state espionage and cyber war, or simply criminal intent and greed, are among the many motivations for these types of attacks to take place. As the digitalisation of more aspects of everyday life takes place with the implementation of smart city, home, health or mobility services, cyber security risks will only tend to increase.

Cybersecurity is one of the most relevant aspects of digital sovereignty. Without a robust cybersecurity legal framework and cyber defence infrastructure in place, states risk the safety of their own citizens, as well as the protection of intellectual property that is imperative for economic growth and development.

These measures must include investment screening (to spot those cases where boundaries between corporate actors and governments are not clear), as well as control of imports of necessary infrastructure that may be used to illegally transfer data to external governments or entities. Moreover, MSs must be able to count on skilled workers that are up to date on the latest trends of hacking and cyberattacks to ensure full protection against these threats.

Another dimension of cybersecurity is misinformation. Misinformation has proven to be a means for malicious actors to tamper with elections or distort public debate with the objective of creating societal instability. Disinformation through the spread of fake news on social media, and direct manipulation of targeted voters based on user profiling information extracted from platforms such as Facebook (e.g. Cambridge Analytica scandal), are drivers for fragmentation, conflict, and even violence against institutions (e.g. the attack on the US Congress in January 2021, or the attack on the largest Italian trade union confederation in October 2021).

³ [ESAA19001ENN.en \(1\).pdf](#) p.6

Without control of misinformation, the stability and sovereignty of democracies are at stake and subject to constant threats. To protect their digital sovereignty, states should have adequate mechanisms and regulation in place to prevent the spread of misinformation.

1.3 Context: why is digital sovereignty especially relevant in Europe?

1.3.1 Digital Sovereignty within the broader context of reinforcing EU strategic autonomy

Concerns about and actions bolstering digital sovereignty in Europe are a part of a broader effort of bolstering EU strategic autonomy in several fields. Comparatively low investment and growth levels have reduced the EU's importance as a top geopolitical power.

According to Eurostat, more than half of the EU's energy needs are met by imports. Russia is the main exporter to the EU of gas, crude oil and coal, which, in itself, is a geopolitical risk. China is also one of the major exporters to the EU of crucial pharmaceuticals and raw materials that are essential for the sustainability of the EU economy.

In the defence field, the EU has no common army and is therefore strongly dependent on the US and other non-EU NATO states. Some MSs (France is leading this trend) have called for a European Army to defend the EU's interests which, as shown for example, in Afghanistan, are not always aligned with those of the US and other allies.

The digital field is no exception to EU dependence. From being at the forefront of technological development in the 1990s, the EU is now behind the US, China, Japan and Korea in many aspects of technological development. The importance of digital technologies is unquestionable in a world of ubiquitous connectivity that spans almost every aspect of societies and economies. Therefore, being at the forefront of technological development is vital not only for economic reasons, but also to ensure that EU values and the functioning of its democracies are protected in a world of rising geopolitical tensions.

Ensuring digital strategic autonomy is now as important as guaranteeing autonomy in any other field. Refraining from taking adequate measures to reduce dependence, especially on non-democratic partners, may jeopardise the very continuity of liberal democracies.

1.3.2 Mapping the EU's competitive disadvantage in the digital realm

The EU's economy is largely reliant on both raw materials and components that are extracted or produced in non-EU countries. China alone accounts for 62% of all critical raw materials. Around 90% of these materials is used in EU electric or electronic equipment, such as optical fibre or semiconductors.

Production of electronic equipment, such as computers or smartphones and telecommunications equipment in the EU, has fallen behind the US and China, standing at a 6% global market share. Regarding semiconductors, which are a key component of almost all electronic devices, the EU accounts for only 9% of worldwide production, which is now concentrated in East Asia.

The EU also lags behind its competitors in the development and production of information technologies such as cloud computing and AI. The EU has no companies in the top 10 by number of AI patents, despite being strong on R&D in the field (although China has recently surpassed the EU in the number of publications). This is probably due to the low levels of investment in new technologies such as blockchain and AI when compared to its competitors. According to a study by the European Investment Bank, the EU would need to invest an additional €5-10 billion every year to bridge this gap.

The EU is also strongly dependent on China regarding high technology imports. In 2020, the EU had a total high technology trade deficit with China of €84 billion. This is mostly due to the imports of computers and other office machinery, as well as electronic and telecommunications equipment which account for the larger part of the trade deficit (€50 billion).

Regarding cloud storage, the EU has no major player in the field. The US and China share cloud service dominance. Market concentration by the so-called *hyperscalers* (which currently control 75% of the whole cloud market) may lead to higher cybersecurity risks as this information may be accessed by intelligence and law enforcement agencies of both China and the US, and market concentration makes these companies more prone to cyberattacks.

To maintain its status as a credible geopolitical power, and to defend itself against digital threats, the EU must ensure that it reduces its competitive gap with other players such as the US and China. The next section provides an overview of the main initiatives that the EU has put forward to bridge this gap.

2. From the failed Lisbon Agenda to a European digital semester

In the 1990s, the European Union and some of its Member States were a digital power. With the Lisbon Agenda of 2000, the EU aimed to become in 10 years “the most competitive and advanced knowledge economy in the world”. However, it failed, for different reasons, including the methods chosen for it, the lack of enough private and public entrepreneurial élan, a large enough venture capital market, and sufficient advanced technological and digital skills among its population and professionals. In over two decades, the EU has become digitally dependent, not only on the US but on China and other countries. Now, it aims to achieve a level of “digital sovereignty”, or at least autonomy, with a series of goals and paths, and a new system of governance.

2.1 The 1990s

Not so long ago, **in the 1990s, the EU dominated the mobile phone industry (2G and 3G) and networks**, with pre-eminent manufacturers of handsets –Nokia was a world leader– and PCs, **and accounted for 30-40% of global manufacturing output of semiconductors, the essential silicon chips**. In 2021, it is now dependent on foreign companies for many of these technologies, so much so, that the MSs and the EU institutions, especially the European Commission, are engaged in a plethora of European and national strategies to fill this gap and move towards a “European digital sovereignty”, or, at least, “autonomy” (Spain and the Netherlands are jointly pushing the concept and policy of “open strategic autonomy”⁴, that is non-protectionist). What has happened in between, and what is the outlook for the future, for what Brussels calls a new “European digital decade”?

In 2000, when it approved the flawed Lisbon Strategy⁵, the EU proposed to turn itself, in 10 years, by 2010, into “the most competitive and advanced knowledge economy in the world”. Twenty years later, the more conservative goal is to become “a world leader” in innovation in AI, data economy and its applications, and other technologies. **These days, in a much broader global market, it makes less than 10% of chips and aspires to a 20% global market share by the end of the decade, imports almost all its mobile phones, has fallen behind in 4G technology** (though less on infrastructures and connectivity), **and is dependent on others for 5G, not to mention its super-dependency on the US and even Chinese platforms**. What went wrong? And what is being done to rectify the situation?

⁴ Non-paper on strategic autonomy while preserving an open economy. 2020.

<https://www.permanentrepresentations.nl/documents/publications/2021/03/24/non-paper-on-strategic-autonomy>

⁵ https://www.europarl.europa.eu/summits/lis1_en.htm

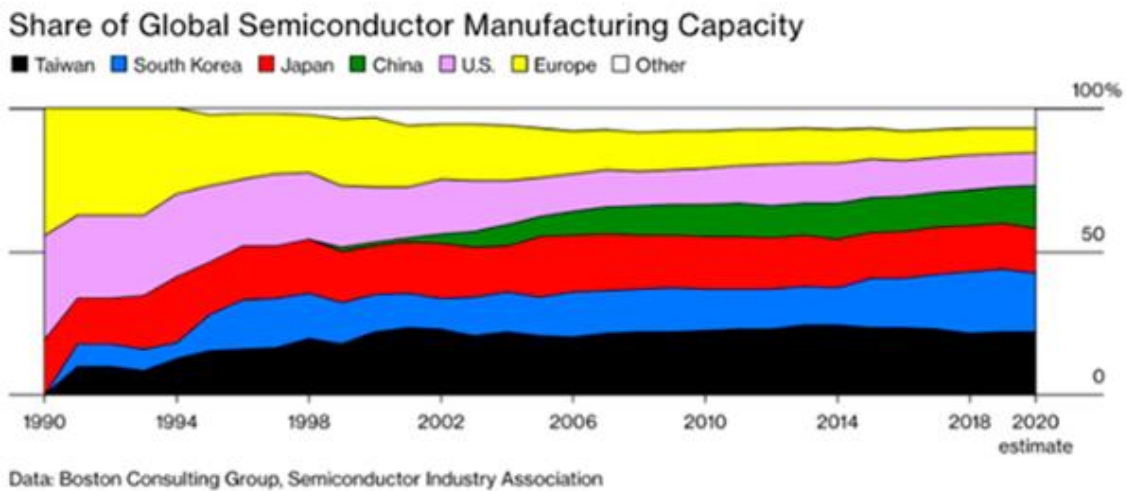


Fig 1: Share of global semiconductor manufacturing capacity, Bloomberg Businessweek⁶

2.2 Flaws in the Lisbon Strategy

The Lisbon Strategy was approved in times of economic bonanza, with the EU embarking on a “growth and jobs” path, and distracted from the revolution underway of the rise of platforms such as Google, Amazon, Apple, etc. - all non-European. The EU was focused on a new enlargement. There was no single digital market and, at the time, the EU did not see sufficient signs of the coming form of globalisation, especially after China joined the WTO in 2000. The transfer of commodities, financial resources, human capital, information and physical products across the world became much easier and much cheaper. It followed the wild offshoring driven by the predominant neoliberal thinking. In the case of China, an important part of its R&D is linked to the manufacturing experience brought about by the European, US and other investments.

The Lisbon Agenda, approved in March 2000 in a time of prosperity, was flawed, not because of its aims, but because of its methods and instruments. Technology was not at its centre, despite European citizens quickly adopting new ITC products and the fascination of European analysts and governments with the “new economy”. Only small and advanced countries, such as Finland and Sweden, were really alert to the consequences of change and the need to react.

The agenda set intermediate targets for the MSs that were not obligatory, nor enforceable or accountable, and failed to provide the public and private resources to attain them. It also lacked an integrated digital market in which European companies could have flourished, while the US and Chinese companies took advantage of the situation.

⁶ Bloomberg Businessweek (March 3, 2021)

<https://webcache.googleusercontent.com/search?q=cache:Yw26Owi0NdEJ:https://www.bloomberg.com/news/articles/2021-03-03/chip-shortage-taiwan-south-korea-s-manufacturing-lead-worries-u-s-china+&cd=1&hl=es&ct=clnk&gl=es>

The so-called Open Method of Co-ordination (OMC) that it had chosen included mainly indicators, benchmarking and peer pressure. However, the Lisbon Agenda had nothing to say about the optimal level of investment in, for example, higher education or R&D. It also did not include common investments (as now with the NextGeneration Funds), nor enforceable or, at least, overseen by the EU, national investments.

As Börje Johansson, Charlie Karlsson, Mikaela Backman and Pia Juusola⁷ saw at the time, due to the lack of results, the Lisbon Agenda, in its revision of 2005, was forced to change some of the implementation processes. Based on the Kok Report, which saw an overloaded agenda, poor co-ordination, conflicting priorities, and the lack of determined political action, the many quantitative goals were reduced, and only the one to dedicate three percent of GDP to R&D remained as in the original set up. The Kok report suggested an improvement in OMC, peer pressure, and benchmarking, a better use of 14 key indicators, and a refocusing from long to mid-term objectives and policies⁸. Still, it did not work, and the EU lagged behind.

2.3 The US, more of an entrepreneurial state and society than the EU

Europe undoubtedly missed the boat, which sailed laden with a substantial cargo of industry and services linked to the Internet (invented at CERN, the European Organisation for Nuclear Research, but also pushed decisively by DARPA, the US Defense Advanced Research Projects Agency). The US, on one side, and China on another, almost by stealth, jumped on the Internet wagon, and developed large online platforms (Alibaba, Google, Amazon, Facebook, Apple and Microsoft amongst others), and the smartphones (the first, the Apple iPhone, went on sale in 2007), and the data economy, with large data centres now in the hands of large non-European operators, including Amazon, without which many European companies would not have been able to get off the ground.

The US owes part of its success to the input of the government, especially the Pentagon, as Marianna Mazzucato convincingly argued in *The Entrepreneurial State* (2013). DARPA, founded in 1958 in response to the Soviet Sputnik, lies behind many of the tech advances of recent decades. Rather than trying to guess the future, it may be said to have invented it, ranging from part of the Internet to touchscreens, GPS, voice interfaces and other innovations, including the new mRNA vaccine system subsequently developed by Moderna, then a small company that had DARPA's backing. Breakthroughs such as these have subsequently been incorporated into money-spinning devices and services. As an example of US public-private dynamism, Steve Jobs was able to reap the

⁷ Johansson, Börje, Charlie Karlsson, Mikaela Backman and Pia Juusola (2007). "The Lisbon Agenda from 2000 to 2010". CESIS. Electronic Working Paper Series. Paper No.106. <http://www.diva-portal.org/smash/get/diva2:487429/FULLTEXT01.pdf>

⁸ Kok, W., et al. (2004), *Facing the Challenge. The Lisbon Agenda for Growth and Employment*.

Report from the High-Level Group, European Commission, Brussels. <https://op.europa.eu/en/publication-detail/-/publication/88b6bc81-e3ad-4156-960f-f549369aa9d4>

Lisbon European Council, 15 July, 2005, Presidency Conclusions <https://data.consilium.europa.eu/doc/document/ST-10255-2005-REV-1/en/pdf>

benefits of these innovations. And ARPAs (without the defence element) are now proliferating in the US Administration (on domestic security, intelligence, energy, recently on the environment, and President Biden wants another to cover health issues).

Various governments, although not the EU as such (there is a European Research Council for Basic Science), are studying the creation of European DARPA or ARPAs (as is Japan), although less closely linked to security concerns. Naturally, this includes the UK, outside the EU, with its Advanced Research and Invention Agency, and Germany, with its civilian Federal Agency for Disruptive Innovation (SPRIN-D) and another for cybersecurity. As *The Economist*⁹ points out, however, such initiatives are doomed to fail unless they are created with the same spirit that motivated DARPA, which means few bureaucratic hurdles, minimal political interference, ample funding (DARPA's 2020 budget was US\$3.6 billion), taking risky gambles and ensuring that all work is contracted out.

There are some exceptions. Two European companies, Nokia (Finland) and Ericsson (Sweden) dominate 5G radio and core access technology but are more expensive than their Chinese and South Korean competitors. It is a sector that Europe does not control, although it is well advanced in the installation of networks and is essential for the Internet of Things (IoT). Another shining example of European know-how is the unique and indispensable machines made by the Dutch firm ASML (each costing €130 mln) for creating nanocircuits in silicon chips¹⁰.

2.4 R&D, from lab to market

Linked with the former issue, one problem of Europe is the transition from scientific research and basic technology to a commercial or other kind of applications, from the lab to the store. R&D in the EU-25 was ahead of the US and Japan in the early 2000s. The EU (25) produced 1.49 science and technology articles per one million US dollar R&D expenditure compared to 0.82 for the US and 0.60 for Japan¹¹. But the translation to applications is lagging.

Europe does not fare badly in the area of basic research. However, the EU concentrates on it, and too little on applied R&D, a situation it is now trying to change. In terms of R&D expenditure, both public and private, there was a gap to the disadvantage of Europe. In several EU MSs, private expenditure on R&D as a share of GDP was substantially below the OECD average. H2020 and European Horizon Programmes have improved the situation, but European knowledge tends to go to other developers. Less than 5% of the European Commission's total budget was devoted to RTD

⁹ *The Economist*, June 5th, 2021: "A growing number of governments hope to clone America's DARPA".

<https://www.economist.com/science-and-technology/2021/06/03/a-growing-number-of-governments-hope-to-clone-americas-darpa>

¹⁰ <https://www.nytimes.com/2021/07/04/technology/tech-cold-war-chips.html?referringSource=articleShare>

¹¹ Archibugi, D. and A. Coco (2005), "Is Europe Becoming the Most Dynamic Knowledge Economy in the World?", *Journal of Common Market Studies* 43, 433-459. http://www.danielearchibugi.org/downloads/papers/2017/11/Archi-Coco_JCMS.pdf

(Research and Technological Development) and less than 6% of the total amount spent by EU governments is on this field¹².

In the field of AI, for instance, the Center for Data Innovation¹³, with an index based on a range of parameters, calculates that the US still leads with 44.6 points out of a possible 100, followed by China with 32 and the EU with 23.3. The Asia Centre¹⁴ argues that Europe fails in five aspects essential for developing a powerful AI sector: an abundance of data, innovative entrepreneurs, talent (high-quality AI scientists and technicians, many of whom have left Europe for the US), an AI-friendly policy environment and well-targeted and abundant funding.

Europe also defined standards, more than now in spite of the so-called Brussels Effect and the GDPR, another instance of regulatory setting by Europe. In fact, European standards industry associations have more seats in the ISO (International Standardisation Organisation) and the IEC (International Electrotechnical Commission) than the USA¹⁵.

Another factor is that the lobbies outside Europe have been able to act again and again to reduce European sovereignty and in Brussels they are an almost unstoppable legal assault force

2.5 The insufficient European venture capital market

Apart from a single digital market and the issue of applied R&D, the **EU also lacked, and still lacks, a large and flexible enough European venture capital market. Many European companies have had, and continue, to go to the US in search of funding, because Europe lacks a single market for venture capital, or a Capital Union.** MS markets are insufficient, even if reformed, something Spain is trying to do with its Start-ups Law. It is not that there is no Silicon Valley in Europe, or ever will be. This may not even be necessary since the model is changing. The EU has no equivalent of Sand Hill Road, the Palo Alto address of numerous venture capital investors, earning it the nickname of the Wall Street of the Valley. Then, of course, there is Wall Street itself and NASDAQ for high-tech companies. But aversion to financial risk still predominates in Europe. Failure is not seen, as it is in the US, as a way of learning for the next entrepreneurial adventure.

¹² Sharp, M. (2001), "The Need for New Perspectives in European Commission Innovation Policy", in Archibugi, D. & B.-Å. Lundvall (2001) (Eds.), *The Globalising Learning Economy*, Oxford, Oxford University Press, 239-252

¹³ Daniel Castro and Michael McLaughlin (2021) Who Is Winning the AI Race: China, the EU, or the United States? — 2021 Update. Center for Data Innovation. <https://www2.datainnovation.org/2021-china-eu-us-ai.pdf>

¹⁴ Thomas L. Oomen (2021): "Why the EU lacks behind China in AI development – Analysis and solutions to enhance EU's AI strategy". Asia Center. <https://centreasia.eu/why-the-eu-lacks-behind-china-in-ai-development-analysis-and-solutions-to-enhance-eu-ai-strategy/>

¹⁵ At ISO: Agencies from EU MSs hold 369 secretariat positions compared to only 104 from the US. At IEC: EU holds 111 positions, and the US just 26.

Link (p.12): <https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320-1.pdf?dimension1=anna2020>

Nonetheless, Europe is improving in this respect. Venture capital funding in Europe has grown six times over the last decade, to nearly \$24 billion in 2020 (\$34.3bln in 2019). This is still short of the record \$73.6 billion the US ecosystem raised in 2020, but a big jump¹⁶. The case of France/Paris is interesting as Macron has managed to position itself with public-private collaboration and improved the situation during the pandemic¹⁷.

2.6 Management of skills, skilling and reskilling

The aspiration to EU digital sovereignty also implies a control of the tech skills, an issue that was not sufficiently taken in account by the Lisbon Agenda. And the EU is lacking skills in this field, especially at the higher end. Though the differences are not that big, there are large gaps between EU MSs.

According to the I-DESI¹⁸, in 2018, EU27 Member States had an average of 0.0056 % their employees in telecommunications. The average for non-EU countries was 0.0052 %.

EU MSs, on average, had 4.3 % of graduates in ICT in 2018. Five of the 18 non-EU countries had a lower proportion of graduates in 2018. The average for non-EU countries counted in the I-DESI was 4.0 %. In 2018, the top four EU MSs, on average, had 6.45 % of graduates in ICT. Only one non-EU country (USA) had a high proportion of ICT graduates.

There is an increasing demand for STEM graduates in Europe. The recovery from the Covid-19 pandemic and the green and digital transitions have further increased the need for STEM skills in Europe, essential for these transitions. In the EU we see in engineering, manufacturing and construction-related studies 15.2 % of graduates and 15.8 % of students, while in natural sciences, mathematics and statistics 6.4 % of graduates and 7.2 % of students¹⁹, with a large gender gap. While there has been an improvement over the years, it is still insufficient compared to the US or China. The graduates in STEM, construction and manufacturing specialisations have increased only from 19% in 2015 to 20.8% in 2019, before the pandemic²⁰.

Europe is not only competing with the US but in caught the middle of a US-China competition and, with Brexit, it has lost the UK, one of its pillars in this field. **To which should be added a STEM gender gap, with less women in the field. The rivalry is not only with the US, but increasingly with China.**

¹⁶ Isabella Pojuner and Freya Pratty (2021): "The data: European vs US VCs". *Sifted*. 3 May 2021. <https://sifted.eu/articles/europe-us-vc/>

¹⁷ See: Alexandre Dewez (2021): «The State of the French Tech Ecosystem in 2020», Overlooked. <https://alexandre.substack.com/p/-the-state-of-the-french-tech-ecosystem>

¹⁸ I-DESI 2020. <https://digital-strategy.ec.europa.eu/en/library/i-desi-2020-how-digital-europe-compared-other-major-world-economies>

¹⁹ Eurostat: Tertiary Education Statistics (2021): https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Tertiary_education_statistics#Fields_of_education

²⁰ https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=educ_uoe_grad04&lang=en

As another report²¹ says, “the United States appears to have offered more programs specialized in AI than any other geographic area, although EU27 comes in a close second in terms of the number of AI-specialized master’s programs”. That also implies the capacity to attract talent from abroad. The majority (64.3% in 2019) of the US AI PhD graduates are from abroad, and they stay (81.8%) in the US. More generally, while it has decreased in some European countries, the number of post-secondary STEM degrees attained by foreign students has grown in the US in the past few decades, increasing by 315% (from 27,470 to 114,092) from 1988-1989 to 2016-2017²². Graduate degrees, particularly Master’s degrees, account for the largest share of STEM degrees awarded to foreign students and have also experienced the fastest growth in recent years in the US, according to the Congressional Research Service²³.

According to the National Science Foundation’s 2017 survey of STEM doctorate recipients from U.S.²⁴, 72% of foreign doctorate recipients were still in the US 10 years after receiving their degrees. This percentage varied by country of origin. For example, STEM graduates from China (90%) and India (83%) stayed at higher rates than European students (69%), though a large number of the latter still remained.

This was something un foreseen in the Lisbon Agenda, but that is dealt with in the new Digital Decade outlook. The Commission proposed a Digital Education Plan for the EU in 2018 (and the MSs are also drawing up national plans) for increasing STEM graduates and fostering entrepreneurial and transversal skills and closing the worrying gender gap in this field. In 2020, a renewed version, a “European Skills Agenda for sustainable competitiveness, social fairness and resilience” was presented, setting ambitious, quantitative objectives for upskilling (improving existing skills) and reskilling (training in new skills) to be achieved within the next five years, for the general public and for specialists²⁵.

2.7 European renewal?

The attempt to establish or restore European digital sovereignty, or at least autonomy, has led to a host of national and Europe-wide strategies. **The European Commission has launched a flurry of proposals including the Digital 2030 Digital Compass and Horizon Europe, to tap into the funds now available through Next Generation EU and the Multiannual Financial Framework 2021-2027, the Path to the Digital Decade, the Chips Act, and the European Digital Decade 20% of the more than € 2 trillion total of the European recovery funds will be spent on innovation and digitalisation over this period.** It is a lot. However, it is also not very much compared with the Biden Plan in the

²¹ Artificial Intelligence Index Report 2021 (Stanford University). https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf

²² The most recent year for which data are available

²³ Congressional Research Service “Foreign STEM Students in the United States” <https://crsreports.congress.gov/product/pdf/IF/IF11347>

²⁴ <https://www.nsf.gov/statistics/srvydoctoratework/>

²⁵ <https://ec.europa.eu/social/BlobServlet?docId=22832&langId=en>

US, or what China is thought to have spent. Getting an advanced semiconductor factory (or ‘foundry’) up and running requires an investment of at least € 20 billion. The German Economic Affairs Minister, Peter Altmaier, wants to invest in chip manufacturing, alongside other European countries and the Commission, as in the US, with 20%-40% state funding. The European Commission has its own plan for semiconductors, where disruption to the supply chain has forced various car plants to grind to a halt. It has also unveiled plans for a European data industry. MSs have woken up to the need for Europe to be sovereign and independent, or at any rate more interdependent, in these areas.

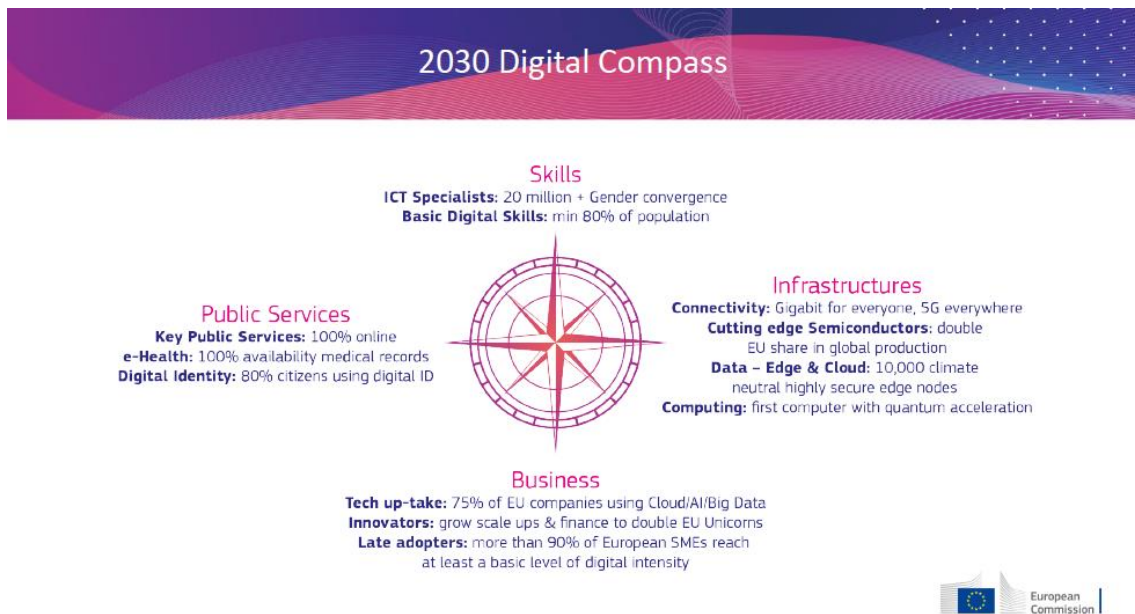


Fig 2: 2030 Digital Compass, European Commission

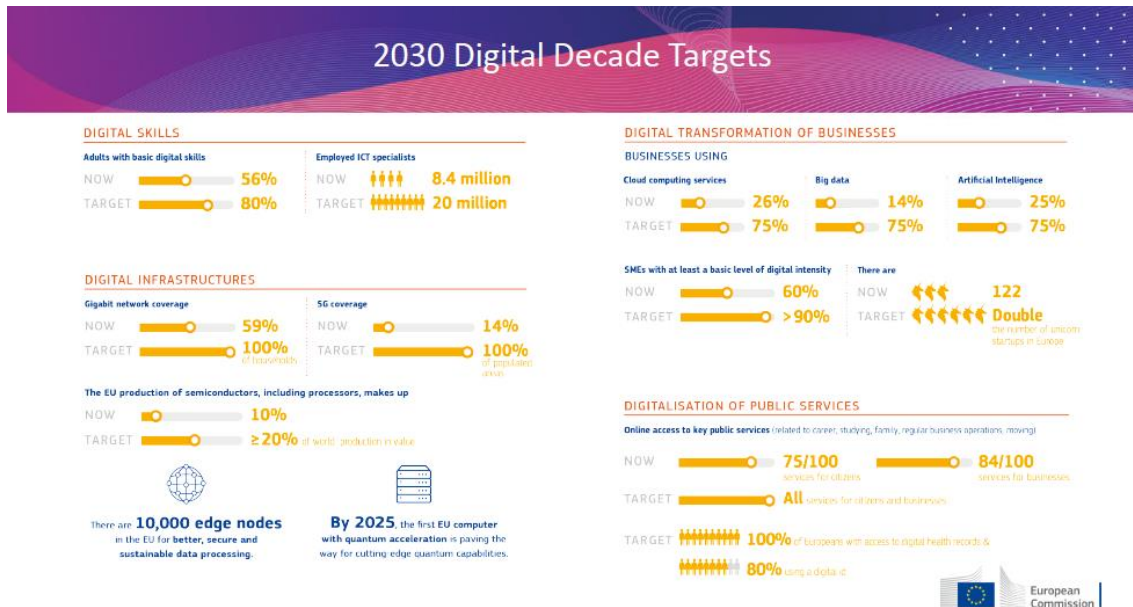


Fig 3: 2030 Digital Decade Targets, European Commission

2.8 From the OMC to the Monitoring and Cooperation Mechanism

The EU has introduced several new instruments, some before the pandemic, some after. Amongst the former are the IPCEIs, that have revealed to be even more important post-pandemic. **The "Important Projects of Common European Interest" involve more than one EU MS and a broad R&D&I ambition.** They promote projects with an impact for the Union and for countries. **They are a key strategic instrument for the implementation of the EU's Industrial Strategy,** and yes, they are a tool to circumvent the limitations on state aid in the EU, so they are useful if there is public money (up to 50%) to invest in them. **An IPCEI brings together knowledge, expertise, financial resources and economic actors across the Union to overcome important market or system failures, including societal challenges, that could not otherwise be addressed.** IPCEIs are large-scale European consortia in key strategic value chains with closely connected business projects. IPCEIs have projects focused on research and development as well as first industrial deployment (FID). There are several IPCEIs running or being structured. For instance, the IPCEI in Microelectronics is divided into five technological fields: energy efficient chips, power semiconductors, sensors, advanced optical equipment and composite materials. The IPCEI enables participating countries to support transnational cooperation projects with important synergies in microelectronics, maintaining and further extending European competences in this field. It also ensures that the entire microelectronics value chain is reliably available to local actors²⁶.

²⁶ <https://www.ipcei-me.eu/what-is/> y <https://www.ipcei-me.eu/what-is/project-structure/>

But perhaps, the most ambitious project of the European Commission, after the EUNextGeneration Fund, involves the proposals for technological itineraries for the EU and its MSs and a proposal of decision²⁷ by which Brussels (Council, Commission and Parliament) would monitor the advancement of each MS towards the goals of the digital decade. This is more than a system of “peer review”, and goes well beyond the OMC of 20 years ago. Each country would draw up an itinerary, a National Digital Decade Strategic Roadmap. In addition, the running of multi-country projects, based on the idea that investment projects, with the necessary scale and critical mass, is “essential to enable the industry to be at the cutting edge of innovation and compete globally, and for the Union to enhance its digital sovereignty”.

The proposed decision sets digital targets for 2030 based on “four cardinal points”: digital skills, digital infrastructures, digitalisation of businesses and of public services. It would be a kind of “European Digital Semester”, in line with the system of the “European Semester for the Economy”.

The starting point is the need for common governance and coordinated investments. The Commission would annually report on the progress of the “Path to the Digital Decade” to the European Parliament and the Council via a “Report of the State of the Digital Decade”. This report, in turn, would trigger a monitoring and cooperation mechanism between the Commission and the MSs. Progress towards the targets at Union level will be monitored via the Digital Economy and Society Index (DESI). Due to the relation of the economy to the digital and to industry, there will perhaps be a need to enlarge the scope of the proposed system.

After the effort made with the NextGeneration Fund, dedicating 20% to digitalisation, the proposals exclude new Community funding, but foster multi-country investments. The system would also be a way of controlling the implementation of the common recovery funds. The proposal involves new powers for the EU institutions, not foreseen in the Treaties, and a larger role for the European Commission. Thus, it will probably be resisted or watered down by some MSs and the European Parliament, but it is much more explicit and governance-led than the Open Method of Coordination.

²⁷ Proposal for a Decision of the European Parliament and of the Council establishing the 2030 Policy Programme “Path to the Digital Decade” Brussels, 16 September 2021

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=consil%3AST_11900_2021_INIT

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11900_2021_ADD_2&from=ES

3. Harnessing European Public-led initiatives with the private sector

3.1 European Union's external dependence and the scenario of European technology companies

Technology innovation has become a new asset of geopolitical competition. Either the global race only involves the US-China rivalry, or Big Tech is included in the increasing debate on whether they have become (Bremmer, 2021), or not (Walt, 2021), shaping forces of the global order, but, in any case, the European Union is lagging behind in the race.

However, technology competitiveness in the geopolitical arena needs to be analysed beyond the big picture. When a specific piece moves, it may overtake the rest. According to a DGAP's survey (Sahin & Barker, 2021), European stakeholders from the private, public and civil sectors are worried about the EU's overdependence on foreign-owned technology providers.

The main reasons involve the lack of a first-mover advantage of European companies and the absence of dominant technology firms in specific areas; the non-availability of venture capital investment; and insufficient and ill-targeted commercialisation of research (technology transfer). However, surveyed stakeholders showed that Europe has four instruments where the EU has a comparative advantage and may leverage its global capacity to act in the tech race. This is the access to the large EU market, its global regulatory power; standard-setting and its data access and control.

This doubled-edge scenario on the role and leadership of companies originating in the EU opens up the debate on whether it is up to the public sector - the EU and its MSs - to support its indigenous companies through public-led initiatives, or whether the European private sector needs to embark on its own way.

To respond to this question, again the stakeholders' survey shows that the **technology area mainly holding back Europe's capacity to act in the global tech race with its own European companies is cloud computing**. This area appears to be the one where experts perceive the EU has the most dependence on external actors (43.9% strongly agree with this idea, while other dependences are perceived as less strong, such as the case of AI where only 21.8% of experts think about a high degree of external dependence). Additionally, cloud computing is also the area where the dependence on a single country is the highest - 93% of experts perceive the EU relies only on the US for cloud computing.

In this picture where cloud computing is the highest dependent technology from other countries compared to any other technology area in the EU (more than AI or high-performance computing), and is also the area with the highest degree of dependence on a single country -the US. Therefore, **it is not by chance that cloud computing has been the technology area where the EU, although**

most particularly its MSs, have mainly tried to foster public-led initiatives to support European firms through governmental coordination, funding, or pooling.

3.2 Cloud computing as the leading example of public support for private firms: the quest to leverage Europe's global capacity to act in the tech race

The EU-wide narrative on European technology sovereignty or strategic autonomy has changed over time. During the previous decade, the 2010 Communication *A Digital Agenda for Europe* had been released to foster several realms of tech governance, such as equal access to web services and content, Internet neutrality, or a larger number of rules for Internet Service Providers (ISPs). It was in 2015 with then-President Juncker's 2015 *A Digital Single Market Strategy for Europe*, when the EU revamped its efforts to shape public-led initiatives affecting the role of European companies, that we can see the reform of telecommunications rules or the simplification of e-commerce rules.

It was not until the current President of the European Commission, Ursula Von der Leyen, that the importance for the EU to become a global tech player was announced and consolidated as such, although Juncker had already proclaimed in 2018 that "the hour of European sovereignty" had come (Juncker, 2018). Her State of the Union speech in 2020 (EC, 2020) mentioned the cloud only once, referring to the announcement to build a European cloud as part of NextGenerationEU funds. In the State of the Union speech in 2021 (EC, 2021), there was no mention of cloud computing. However, support for European companies was a part of the 2021 speech, involving pooling resources and integrating them into the two mechanisms which had been created - IPCEIs (Important Projects of Common European Interest) and new European Alliances, created with the updated Industrial Strategy from May 2021.

Attention to cloud computing has mainly been given at the MS level. The importance of fostering EU-based cloud technologies is key, not only to creating competitive firms and fostering existing ones, but also because **cloud computing touches on a core idea of European technological sovereignty - European data to be gathered, processed and used by Europeans, for Europeans, and from Europe. It refers to personal data, but also to industrial data** and how cloud computing may help the proposed European data marketplaces to make endogenous sectors more competitive in strategic sectors from health and manufacturing to telecommunications and green technologies by using a European cloud.

This is of special importance for the EU and its Member States. The main challenge is the fact that **cloud computing favours large first-mover companies** as they are able to consolidate from the very beginning path-dependent service relations with their users. Once a cloud computing system is established and is spread across companies and public institutions, **the portfolio of offered services is thinner** and largely depends on what is offered by this cloud computing company. Also, **data**

interoperability and portability are harder as all data a client aims to share with others needs to indispensably go through the same cloud.

Currently, the public sector is supporting the development of GAIA-X, which is presented as a cloud data infrastructure aiming to become the starting point of a European data ecosystem. However, at present, the European cloud computing landscape is mainly dominated by US providers, namely Amazon, Google, IBM and Microsoft. Some MSs have been able to develop their own cloud providers - the two French OVHcloud and Orange, and the German Deutsche Telekom-, but the number of clients and its continental presence is more limited.

To analyse both the opportunities and weaknesses that the GAIA-X may have as a launching point to leverage European technology sovereignty, **it is important to analyse what attempts had been carried out in the past by European governments to identify policy lessons, in terms of successes and failures, which may serve as useful recommendations for the ongoing GAIA-X project.**

3.2.1 Lessons from the past: “sovereign” cloud computing projects in Europe

Previous European attempts to gain ground in the cloud computing arena were unsuccessful. It is usually said that main limitations to being competitive in cloud are the lack of capital-intensive infrastructure, the absence of large networks of data centres, and the shortage of a talented workforce. This is partially true, but reasons cannot be limited to these three factors.

France and Germany (the same countries which launched the GAIA-X project in 2020) have been the EU MSs to have mainly worked on developing their own projects.

These include, in France, the *Andròmede* sovereign cloud project created in 2009, in Germany, the *De-Mail* tool for secure communications with an alternative email residing in a sovereign cloud, and, finally, a French-German *Quaero* initiative to build up a European search engine whose data would be collected in a European cloud.

In 2009, **the French government launched the *Andròmede* project**, a sovereign cloud which was designed to lead the construction of a large data hosting centre supported by a €150 million state-funded budget. It was funded via *Le Grand Emprunt*, a government-led borrowing initiative to support infrastructure modernisation and the creation of an innovative ecosystem. Initially, *Andròmede* was seen as a project rooted in national security issues, as the growing US cloud computing advances were seen as a risk to the French law which protects certain types of information and must be held within France. National sovereignty was the backbone to the project, but the national security concern evolved into an issue of economic competitiveness, as recognised by the then-Prime Minister, François Fillon, in January 2010 (Vie Publique, 2010).

Once the economic competitiveness concern was prioritised, an open call was launched to seek an implementing company. Orange/France Telecom and Thales appeared as the main candidates, alongside other companies, and, in 2011, the €150 million state-funded budget was designated to a public-private partnership with Orange/France Telecom, Thales and Dassault Systèmes. However, operators differed in procedures for secure data hosting, and **the government ended up splitting the initially foreseen single project into two competing projects** (INPLP, 2020) - Cloudwatt (initiated by Orange and Thales) and Numery (supported by SFR and the IT group Bull). Each received the €75 million, and they had to compete to offer the most competitive national secure data hosting platform to the government.

Both projects failed. **Policy failures were not related to technical issues, but to limited coordination with the government and lack of communication from larger companies developing the project for SMEs, the latter being the targeted actors expecting the national cloud project to be launched and to benefit from it.** Orange and Thales, on the one hand, and SFR and Bull, on the other, ended up joining forces because they considered each other to have resources which were solid, well-advanced, but especially complementary. Companies also had a large number of talented workers and skills being interoperable when one company needed the other's help. This was true.

Limitations lay in the fact that each of the two projects acquired a high level of autonomy in the development of the cloud project, communications were not continuous with the government, and engagement and communication with SMEs was limited (ZDNet, 2012). This discouraged SMEs from waiting for larger companies to bring to the market a cloud project - even if sovereign, national-based -, and SMEs and users turned to GAFAM companies from the US. Additionally, **certification of applications generated highly significant costs** which were not reduced, thus slowing down the development of these two cloud projects.

With regards to the **German De-Mail project**, this was not a purely sovereign cloud project as such. Launched in 2012, its initial goal was to introduce a tool for communications to send digital documents securely, confidentially and verifiably. Exchanged data could be hosted in a cloud which was to be secure. This was shown as a sign of force by Germany to foster its own "national technology sovereignty" and autonomy.

De-Mail still exists, but the project was criticised from the beginning due to **three policy shortcomings**.

- **Technically**, it lacked end-to-end encryption, so it does not ensure a fully secure system which might incentivise companies to jump in and use it. Additionally, there is control over whether the DE-Mail provider is secure, but not on whether the actual sender providing the signature of the email is a secure, trustworthy sender.

- **Economically**, it is a paid service whose costs were similar to physically sent methods -so users would still opt for either remaining in free email platforms, or sending physical letters when needed.
- **In terms of communication**, the platform is not user-friendly. Official documents state that there is about a million private customers, roughly 10,000 SMEs and 1,000 large companies registered. However, there is **no publicly available information on active users -not only registered- and intensity of emails exchange**. User acceptance is an important factor when it comes down to maintaining a system which still exists since its creation in 2012 (Boukal, 2019).

The story of the **Franco-German Quaero initiative** is worth analysing for policy failures. *Quaero* was projected to be an alternative search engine to its rival, Google. It was expected to become a Europeanist project which would guarantee two aspects: the protection of European personal data, and the guarantee that European users would not suffer from the Chirac-called “information overload” that then-French President said Google led to, with biased prioritised information when searching for information in the search engine. European values were the *raison d’être* to create this project (DW, 2006).

The *Quaero* initiative was unsuccessful due to two main reasons. Firstly, it was criticised by the private sector for being a **government-funded project which could have delayed the development of the project. Whether or not this is true**, this criticism led private companies to be discouraged from joining the project. Secondly, **French and German companies did not agree on resource-sharing** for the development of the project. France and Germany had high ambitions, as they aimed to incorporate not only text in the search engine, but also images and audio clips to search for information.

In conclusion, three previous attempts led by MSs have proven so far to be unsuccessful. **There is no single, one-stop set of reasons to explain this**. Each project had its own policy failures, **although public-private communications and user-friendly interfaces appear to be two of the most important ones**.

However, the fact that these attempts have been unsuccessful **does not mean that current initiatives will end up following the same path and with the same results**. In fact, the objective of this analysis is to paint a picture of the policy lessons from the past to render current attempts more effective and have a constructive upwards trend in terms of operationalisation, communication across sectors, and mutual understanding.

3.3 Current attempts to revamp European technology sovereignty through public-led initiatives on cloud computing

Cloud computing has received a lot of attention since 2020. This matches with the European Commission President, Ursula Von der Leyen's approach to the *European Digital Decade* which started last year. On 4 June 2020, the German Economy Minister, Peter Altmaier, announced the launch of GAIA-X, a cloud data infrastructure which is expected to become the starting point of a European data ecosystem (Jorge-Ricart, 2020). The EU had already underlined in its European Data Strategy from February 2020 the need for turning the Union into a reliable, trustworthy global partner through the setting-up of data ecosystems, both of excellence and of trust. In this, cloud and data are close partners, and it also matches with IPCEIs and new European Alliances as EU-led proposals.

3.3.1 EU Member State perspectives on cloud computing

GAIA-X is initially a Franco-German initiative and not a EU-led project as such. The cloud initiative aims to provide companies with an alternative to Amazon Web Services, Alibaba or Google. According to the French Economy Minister, Bruno Le Maire: "We are not China, we are not the United States – **we are European countries with our own values and our won European interests that we want to defend**".

The project is seen as the **promise for Europe to regain its "digital sovereignty" and to assert Europe in the world**. As Josep Borrell, the High Representative of the EU for Foreign Affairs and Security Policy, and Thierry Breton, European Commissioner for Internal Market, wrote a few days after the GAIA-X launch in 2020, "the era of conciliatory, if not naïve, Europe has come of age" (EEAS, 2020). According to them, soft power is no longer enough as it needs to be complemented with a "hard power", and not just in terms of military power and defence.

With this statement, they pointed to the need for resilience and autonomy as the pathway for the Union to ensure data and essential infrastructure protection for society, by using a stronger leadership as a Union to contribute to a global system balance.

Much has happened since the launch of GAIA-X in June 2020. At the beginning, **it was intended to simply integrate European companies. However, over time, some US companies have also started entering the project**. On the positive side, GAIA-X has received strong attention, not only from French and German stakeholders, but also from other EU MSs.

To give an example, **the Government of Spain launched the national GAIA-X hub call, and it received more than 180 proposals from 313 Spanish companies, most of them SMEs** (Del-Castillo, 2021). This shows a solid interest to enter a cloud computing project where, in turn, data marketplaces which are being developed by the EU may be embedded, thus having a multiplier

effect for SMEs and potential ties with other companies across the EU. In the case of Spain, more of the NextGenerationEU budget has been allocated to data marketplaces in the strategic sectors of health and tourism (MINECO, 2021).

On the other hand, recent declarations (Goujard & Cerulus, POLITICO, 2021) from industry and government officials involved in the GAIA-X project at the EU level show that the initiative is facing **several obstacles**. First, there is **no consensus on overall goals and resources devoted** to each of them. Second, there has been a **strong internal competition to control a key competence of GAIA-X (which member is in charge of communications with governments)**. Third, there are **delays in agreeing on ground rules on data storage**.

While previous attempts failed due to communication issues with SMEs and governments, the problem with the current GAIA-X is the fighting over who will lead the project and play the role of engaging with governments.

Thus said, **it is important to remark that all technology projects - either created in the EU or in the US or led by governments or by the private sector - have always faced internal fighting and problems from the very beginning**. When the US CLOUD Act was released (Linklaters, 2019), the private sector criticised it as it gives US law enforcement authorities the power to request data stored by most major cloud providers, even if it is outside the US. **Some US companies were against the US CLOUD Act**, and this explains why Apple, for example, rejected US requests to have access to its end-to-end encryption-based data.

Therefore, **the EU is not the only single actor that suffers from delays and limitations in its technology projects. Other countries have also done so**. GAIA-X needs to be analysed from a critical, but also constructive perspective to improve its shortcomings and make it a feasible project. Policy recommendations are included in Section 4.

3.3.2 Policy responses at the EU level

The European Union has launched in recent years a set of measures to support the private sector, also in the cloud computing area. These are IPCEIs and the new European Alliances.

Concretely, **IPCEIs (Important Projects of Common European Interest)** are aimed at supporting MS efforts to pool public resources via this framework in areas where the market cannot alone deliver disrupting outcomes.

In May 2021, 12 EU Member States - Belgium, the Czech Republic, France, Germany, Hungary, Italy, Latvia, Luxembourg, Poland, Slovenia, Spain and the Netherlands- **joined forces to create the proposal of an IPCEI on Next Generation Cloud Infrastructure and Services (IPCEI-CIS)**, which may

create a common cloud and edge infrastructure and its associated smart services for the future (BMW.de, 2021).

This IPCEI will contribute to the implementation of the **High-Impact Project foreseen in the EU Data Strategy**, aiming to “develop data processing infrastructures, data sharing tools, architectures and governance mechanisms for thriving data sharing and to federate energy-efficient and trustworthy cloud infrastructures and related services”. It will also **contribute to the Review of the EU Industrial Strategy** to “strengthen Europe’s industrial position in the global cloud and edge computing market, notably addressing the trend towards increasing distribution and decentralisation of data processing capacities and the need to enable federated and vendor-agnostic cloud ecosystem”.

The main competitors to this newly-founded IPCEI are not only the traditional ones (Microsoft, Amazon Web Services, or Alibaba). **Google has recently announced** that it plans to outcompete these firms by taking advantage of **two new key trends - the multi-cloud and the distributed cloud** (Waters, FT, 2021). The multi-cloud involves leveraging the resources of a number of different public clouds to handle a computing task. This reduces the risk of lock-in by a single cloud supply, and Google will gain ground with its data warehousing service that taps into data held in a number of different clouds, not just a single one. On the other hand, the distributed cloud involves establishing smaller facilities to handle data locally, instead of centralising data computing in large data centres. The goal is to attract locally-based SMEs to their cloud.

Consequently, several policy recommendations are included in Section 4 for the EU-led IPCEI to be effective and feasible.

Along with IPCEIs, the EU has also created and updated **European Alliances**. Some of them were launched with the “Updating the 2020 New Industrial Strategy” Communication released in May 2021, including **the Alliance on Cloud, Edge, and Data**. Official documents show that membership eligibility criteria are specific-framed (in terms of use of data for national security purposes; not contravening public policy interests of the Union; and ownership of intellectual property only on the European territory). This has strong implications on how EU-based private companies will be able to engage with European governments, but especially the scope and breadth of involvement by non-EU firms.

The goal of the European Alliance is **to be able to involve, not only SMEs in relation to large companies, but especially to make a truly cross-border production chain feasible across MSs**. Policy recommendations are included in Section 4.

3.4 Policy opportunities to move European public-led initiatives forward

There is no single solution or set of “formulas” to make European companies competitive in cloud computing, or to consolidate new long-term proposals with specific mandates, timings and allocated resources. However, the following policy opportunities may shed light on how to learn from the past and overcome challenges arising from current initiatives (GAIA-X, IPCEI-CIS, and the Alliance on Cloud, Edge, and Data).

For GAIA-X, these involve:

- 1. Distributing competences amongst the leadership and implementation roles, and engage more SMEs.** GAIA-X has included both large firms and SMEs in the same project. This is a lesson learnt from the *Andròmede* project, which gave control to the largest companies. However, the project should restructure its governance model so it is not taken over by a few large members in the leadership team. If several working groups were created, and the largest companies took the leading role, SMEs should then be given an active role for specific lines of management of the working group - on how to communicate with other GAIA-X working groups, or how to coordinate information-sharing across a project on the value chain.
- 2. Creating inter-working group periodic meetings,** essential to avoid overlapping, but especially to foster mutual trust and confidence, and ensure that national hubs are equally involved in all working groups at the EU level.
- 3. Agreeing on common rules for SME market entry into the GAIA-X outcomes.** Although each MS may vary in the scope and budget allocated to its national hub - as this depends on the number of proposals and interested stakeholders in the national call -, national hubs should agree on common rules for market entry of SMEs into any of the existing GAIA-X national hubs. SMEs from different countries may have complementary assets and resources to create a disrupting product, and this must not be overlooked.

For the IPCEI-CIS, this involves:

- 1. Going fast in setting up a common Multi-Provider Cloud-Edge Continuum.** The IPCEI-CIS initial statement referred to this initiative in order to create reliable and ultra-secure processing capabilities with guaranteed latency and bandwidth. MSs which are part of the IPCEI-CIS should first create a mapping of joint risks as well as of available resources per country, so that each MS may focus on the industry it may have greater interest in or leadership. For example, if Spain, which is part of the IPCEI-CIS, has a strong interest in tourism with the seamless travel and smart cities’ aspects that the IPCEI-CIS mentions, the country should take a role in it. A similar situation may arise with France in the healthcare

sector with edge-augmented operating rooms, as it may leverage this opportunity with the French four 3IA (Interdisciplinary Institutes for AI) which has created across the country.

2. **Fostering interstate cooperation amongst regional innovation ecosystems created within MSs.** While cloud computing may not be the specific case for this at present, there are other technologies which are being strongly developed by sub-state innovation ecosystems (i.e. Baden-Württemberg's Cyber Valley, Europe's largest AI consortium, and Bavaria's Quantum Valley).

For the European Alliance on Cloud, Edge, and Data, this involves:

1. **Incentivizing SMEs with international client portfolios which may significantly contribute to the European Alliance.** Some MSs have leading companies on the open source side of cloud computing. These are typically SMEs, but they have a large investment portfolio with international clients (not necessarily European). The European Alliance may create mechanisms (fiscal incentives, new clients within Europe) to attract them to joining the European Alliance.
2. **Government carrying out an impact assessment of new Big Tech proposals and models of cloud computing on their own public-led initiatives.** Although governments do not directly participate in European Alliances, they are at the core of the industrial policy for each country. Thus, governments should enact an inter-ministerial committee in order to create a joint risk mapping and its impacts on governmental proposals and national companies.

4. Convergence or divergence? Current digital trends in the EU, US and Asia

4.1 Current digital trends in the EU, US and Asia

4.1.1 National digital performance of the EU, US and Asia

Digitalisation offers important growth opportunities, though its developments give rise to many challenges. It is changing business structures, operations and value chains, as well as innovation and international trade. Moreover, the recent Covid-19 pandemic has demonstrated the necessity of digital technology for even the most traditional sectors. However, there is a growing concern about Europe's digital sovereignty since it seems that in certain key areas the EU, and especially the southern areas, remains (significantly) behind other states such as the US or China. In this chapter, we try to describe the digital performance differences of the EU from the US, China and other digitisation leaders.

One of the main indexes to compare country digital performance is the International Digital Economy and Society Index (I-DESI). The indicator tries to estimate the digital economy performance of EU27 compared to 18 other countries worldwide (Australia, Brazil, Canada, Chile, China, Iceland, Israel, Japan, Mexico, New Zealand, Norway, Russia, Serbia, South Korea, Switzerland, Turkey, the UK and the US). **It uses a weighting system of 24 indicators to rank each country based on its digital performance to benchmark the progress of the digital economy and society. The indicator estimation is undertaken against five dimensions:**

1. Connectivity, broadband infrastructure, and quality;
2. Human capital, digital skills;
3. Citizen use of the Internet, activities performed by citizens already online;
4. Integration of Digital Technology, business digitalisation and online sales;
5. Digital public services, digitalisation of public services.

Due to the structural and other differences among EU countries, the performance of Europe is presented as the average performance of: a) the top four performing countries of EU27; b) the EU27 MSs; and c) the bottom four EU27 performing countries. In general, in the five dimensions of the I-DESI 2020, the US score is the highest, while the top four countries of the EU rank second, followed by Switzerland, Norway and Iceland. Unfortunately, the EU average is behind prominent digital countries such as Korea and Japan. Furthermore, a critical issue that should be considered is the great disparities in the EU since the EU bottom four countries rank third from the bottom, right after Mexico.

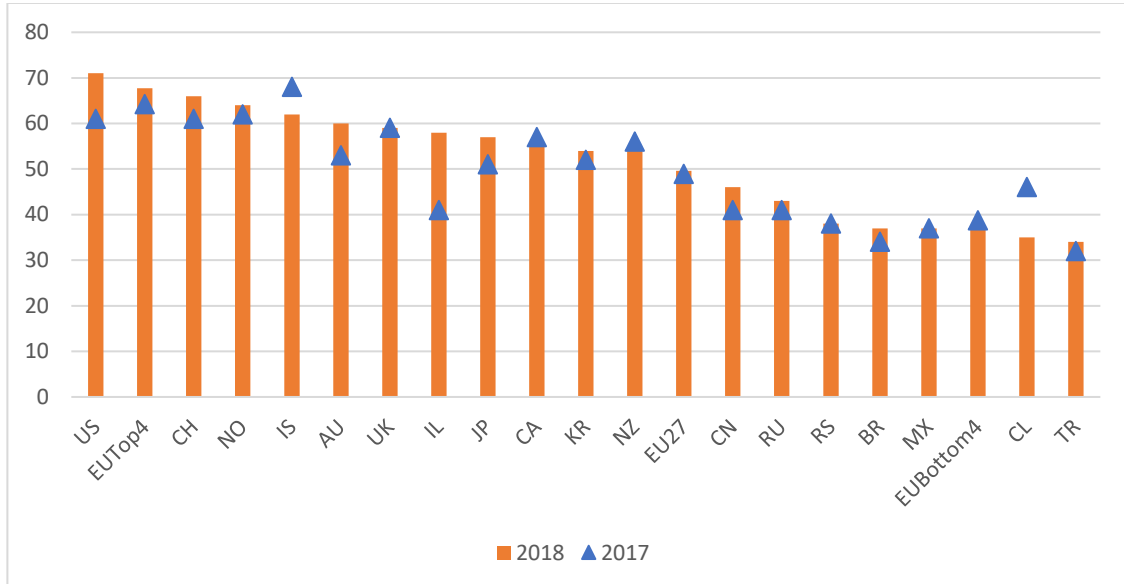


Fig 4: I-DESI index for 2017 AND 2018, European Commission

Japan ranks first in the connectivity dimension, which examines the fixed and mobile broadband deployment and take-up. In 2018, the average score for the leading four EU27 was third after Iceland. The average score for the bottom four EU27 MSs (54.5) was ahead of five non-European countries. In this area, the EU27 average compares well with non-EU countries. The strongest areas in this dimension for EU27 were the Broadband Take-up and Mobile Broadband sub-dimensions. Several of the bottom five non-EU countries (Brazil, Chile, Mexico and Russia) are characterised by substantial size and low population density, making broadband infrastructure distribution challenging and costly.

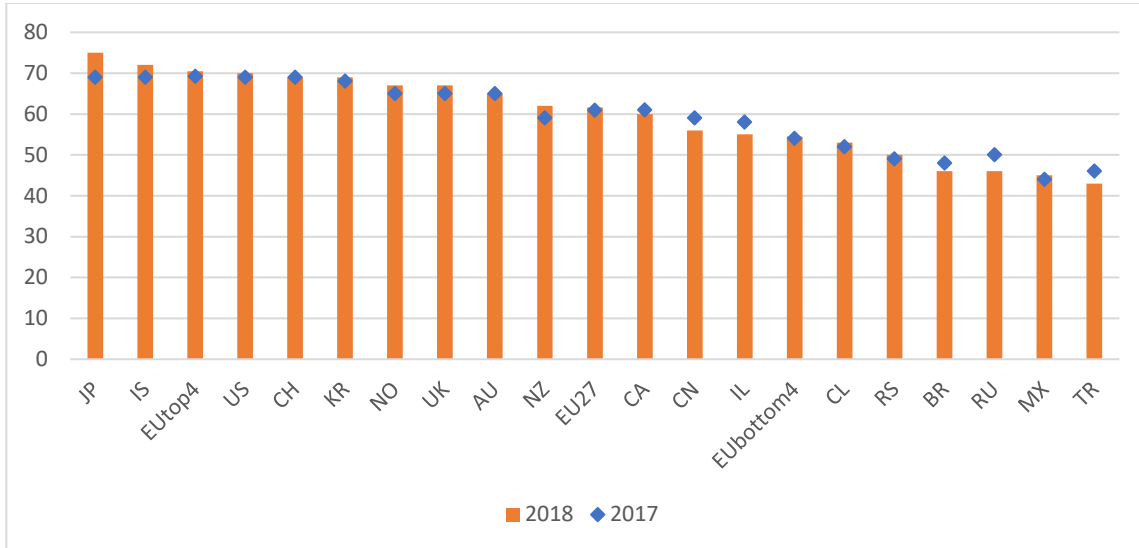


Fig 5: Connectivity dimension of I-DESI FOR 2017 AND 2018, European Commission

The human capital dimension analyses the necessary skills to reap the benefits of digitalisation, such as basic and advanced digital skills and ICT graduates. In 2018, the EU27 average performance was 41.8. Ten of the 18 non-EU countries had a higher score, including the US, Switzerland, China, the UK and Japan. The top four EU27 MS's average score was second in the ranking, while the last four countries ranked almost at the bottom, stressing the great disparities in the EU. During the four years studied in the I-DESI (2015-2018), the average EU27 human capital score improved by 3%, from 38.8 in 2015 to 41.8 in 2018. Instead, non-EU countries increased by 5.9% (37.1% in 2015 to 43% in 2018).

Considering the individual indicators of the human capital dimension, 49.7% of users had basic skills such as word processing in the EU27 in 2018. The top four EU27 share was more than 70%, while Iceland and Switzerland had the same or a higher level of Internet skills in 2018. In basic skills, such as advanced spreadsheet skills, the percentage of the EU27 was 28.7%. In the top four EU27 countries, more than 40% of users possessed basic digital skills. Japan and Switzerland presented the same or a superior level of skills in 2018.

The final indicator refers to users that have at least basic software skills, such as coding skills. The average performance of the EU27 MSs was 5.7%, whereas, in non-EU countries, the average was 7.8%. Regarding the top four EU27, the percentage was more than 10% though Iceland, Japan, Norway, Switzerland and the USA had the same or higher skills levels. Finland and Sweden had the highest percentage of people with ICT specialist skills as well as the highest share of STEM graduates.

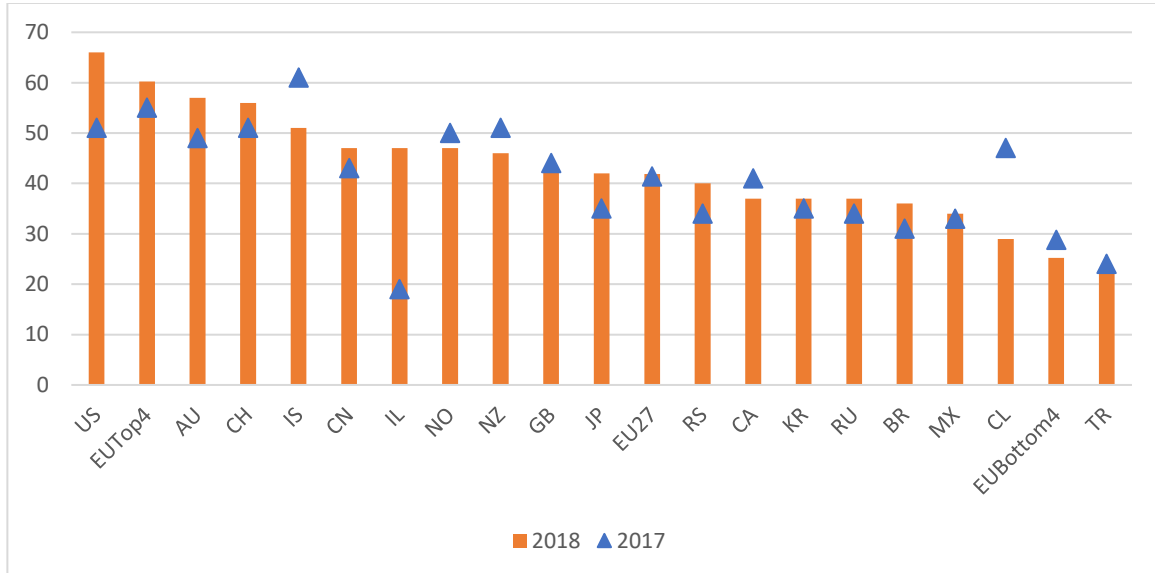


Fig 6: Human capital dimension of I-DESI for 2017 AND 2018, European Commission

The Use of Internet Services dimension examines the use and variety of activities undertaken by citizens online. In 2018, the EU27 average performance was 47, and 12 out of the 18 non-EU countries ranked higher. It was the strongest area for non-EU countries since their average was 51.8. The mean performance of the EU was behind non-EU countries across all four years investigated. The top four EU countries scored similarly to the top four non-EU countries. Again, there were great disparities since the average performance of the EU bottom four countries was almost in the last position of the total ranking. In 2018, the top four EU27 had an average score of 67 and three non-EU countries (Iceland, Norway, USA) performed better than the EU countries. The bottom four EU27 score was 31.4, and only Chile from the non-EU countries had a lower score than these.

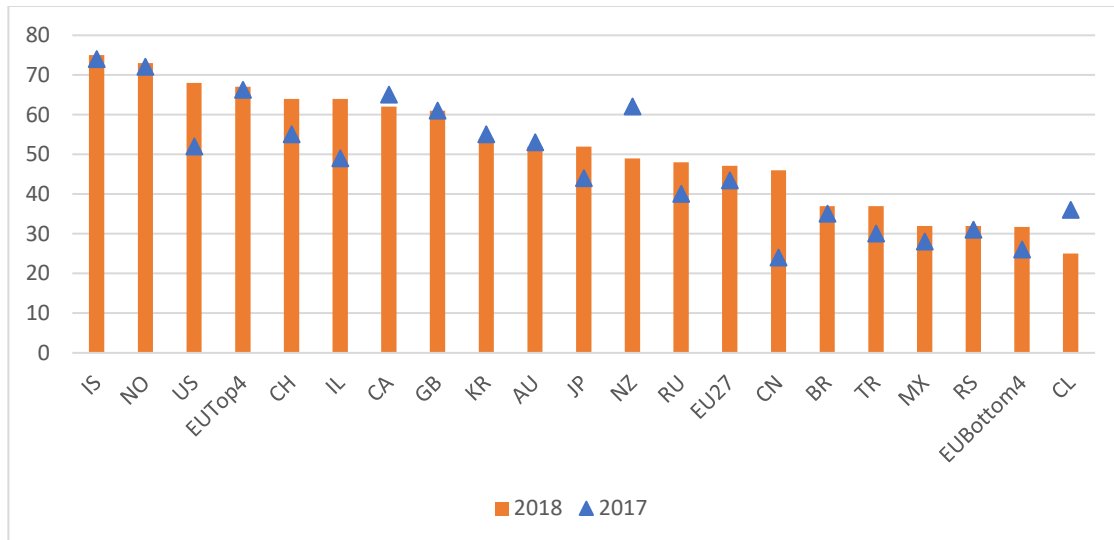


Fig 7: Citizen use of Internet dimension of I-DESI for 2017 AND 2018, European Commission

In integrating digital technology by business, the EU top four countries ranked third, followed by the US. Switzerland and Israel took the first two places. However, the EU average was less than half of the Swiss score and the EU bottom four ranked almost last, before Brazil. The integration of the digital technology dimension considers both the digitalisation of businesses and the development of e-commerce. In 2017, the average EU27 performance drew level with non-EU countries for the first time since 2013. However, the following year, the EU27 slipped further behind again. The average 2015-2018 EU27 Integration of Digital Technology score increased by 2.7% from 38.4 in 2015 to 41.1 in 2018. Over the same period, the increase for non-EU countries was 2.9% (from 43.4% to 46.2% in 2018).

The sub-dimension of Business digitalisation includes two indicators: a) businesses' views about the availability of the latest technology; and b) business technology absorption. For the former, in 2018, the EU27 average score was 51.8, while twelve of the 18 non-EU countries had a better score. The total mean for non-EU countries was 58.8. For the latter, in the same year, the score of the EU27 was 41.8, and eleven of the non-EU countries had a higher score. The overall average for non-EU countries was 47.7. EU firms currently lag behind in adopting digital technologies, mainly in construction and the Internet of Things.

The second sub-dimension is eCommerce, which includes two indicators: a) SMEs selling online; and b) the number of secure Internet servers. During the examined year, in the EU27, an average of 29.1% of SMEs had received orders through the Internet. Still, the average in non-EU countries was considerably higher (43.6%), and 14 non-EU countries exceeded the EU27 average. The EU27 scored 36 in 2018, and surprisingly the average for non-EU countries was 27.9.

The final sub-dimension in this category investigates the number of secure Internet servers per one million people. Secure servers are required to support eCommerce. The normalised average score in the EU27 in 2018 was 36.0, whereas the average performance for non-EU countries was 27.9.

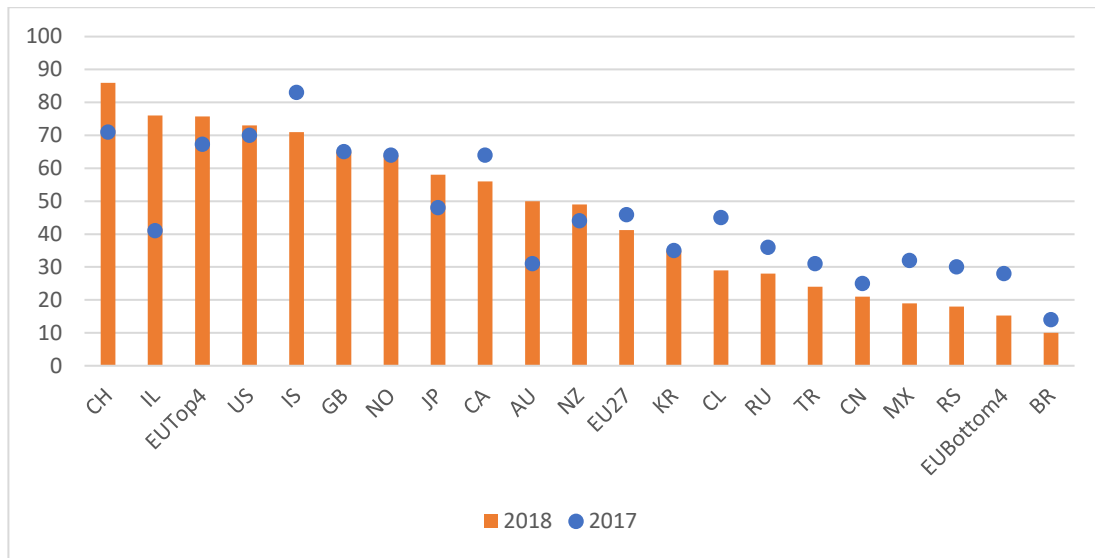


Fig 8: Integration of digital technology of I-DESI for 2017 AND 2018, European Commission

Apart from the I-DESI, the Global Entrepreneurship and Development Institute (GEDI) developed the Digital Platform Economic Index (DPE Index), a country-level composite indicator of the global digital ecosystem. It integrates both the digital and entrepreneurial ecosystem, and includes 12 pillars to combine these two ecosystems for 116 countries. The results are similar to the I-DESI as described above. The GEDI index suggests that four EU member countries were in the first ten countries, with Europe's largest countries - Germany, France, Italy and Spain - ranking in the second cohort. Scandinavian countries (Sweden, Norway, Denmark and Finland) and Switzerland were stronger than the large European countries. The top score of the index went to the US, which is higher than the 14th ranked Germany by almost 25%.

4.1.2 Corporate digital performance of the EU, US and Asia

More mature companies, concerning digitalisation, have a comparative advantage in AI adoption. However, **only two European firms are in the worldwide top 30 digitalised companies, and at the end of 2017, none of the ten largest Internet companies worldwide was based in Europe.** The rapid growth of non-EU technology firms could significantly constrain the development of EU high-technology companies and policy-making at the EU level.

According to McKinsey's 2018 Digital Survey, nearly 80% of European businesses had experienced a positive return on their digital transformation. Still, only 50% realised a return more prominent

than their weighted cost of capital. In addition, **the digital gap between Western Europe and the US remained constant.** There are two main components in the use of digital technologies and its spreading European companies are less mature in spreading digital technologies and the use of those technologies for new services and business models.

The 2020 European Investment Bank Survey (EIBIS) indicated that the increased use of digital technologies **due to the Covid-19 restriction measures** was evident to half of all firms that participated in the survey (bases in the EU and US), mainly due to large firms and firms in the manufacturing sector. **51% of EU firms had, to some extent, implemented at least one digital technology, while the fully implemented was at 12%.** Full implementation was the most widespread among companies in the infrastructure sector (16%), while partial implementation was usual among manufacturing firms (55%). Still, the US performance was significantly more prominent. Differences among EU countries was also apparent, with adoption rates ranging from 47% to 76%. **The manufacturing sector was the leader in digital technology adoption rates both in the US and EU.**

Regarding firm size, 75% of large enterprises had partially implemented a digital technology, while the percentage dropped to 52% for SMEs. The technologies where the US had a significant advantage compared to the EU was in using IOT applications and drones. The EU and US adoption rates were close concerning the use of other technologies, with the EU having a slight advantage in the use of platform technologies.

Dell Technologies surveyed 4,300 business leaders worldwide to analyse their organisations' transformation efforts in 2020. The Dell Technologies Digital Transformation Index (DT Index) is a global benchmark representing enterprises' digital performance globally. Before the recent disruption, the speed of transformation was lagging, making the change in recent months even more challenging. Nearly one in three companies worried that they may not survive the next couple of years, while 60% believed they would survive but decrease jobs and take years to be profitable again. Furthermore, the pandemic accelerated the digital transformation programmes in 2020, since 80% of participant firms fast-tracked some digital transformation programmes in this year. Yet, only half of them (41%) accelerated the majority of their programmes.

Businesses are encountering barriers to the process of transformation, according to the Dell Technologies survey. The main obstacles include data privacy and security concerns, lack of budget and resources, economic growth, in-house skill sets and expertise and immature digital culture. In addition, planned investments over the next one to three years mainly regard foundational technology such as cybersecurity solutions and data management tools. Emerging technology investments follow, such as investments in AI algorithms and commercial/industrial robotics. The workforce digital skills were significantly enhanced, but there is still plenty of room for improvement.

4.1.3 AI trends in the EU, US and Asia

Artificial intelligence is critical since it forms the foundation of computer learning. AI technology advancement is of great help in many scientific fields, from medical breakthroughs to cutting-edge climate change research. According to a recent survey conducted by McKinsey in 2020, organisations use AI as a tool for generating value in the form of revenues. A small group of respondents from various industries attributed 20% or more of their organisations' earnings before interest and taxes (EBIT) to AI. However, AI leaders and the majority of firms are still struggling to capitalise on the technology. This section compares the AI trends of the world's major AI players - China, the EU and the US.

Regarding AI research publications, the number of AI journal publications grew by 34.5% from 2019 to 2020, when the percentage growth from 2018 to 2019 was much smaller (19.6%). In 2020, China exceeded the US in its share of AI journal citations worldwide, temporarily overtaken by the US in the overall number of AI journal publications in 2004 and then retaking the lead in 2017. In terms of peer-reviewed AI publications in 2019, China (22.4%) had the lion's share, followed by the EU (16.4%) and the US (14.6%). Historically, the EU had been the leader in AI scientific publications, however, China made an important leap in the last year, and the EU should now focus on regaining its leading position (Zhang et al., 2021).

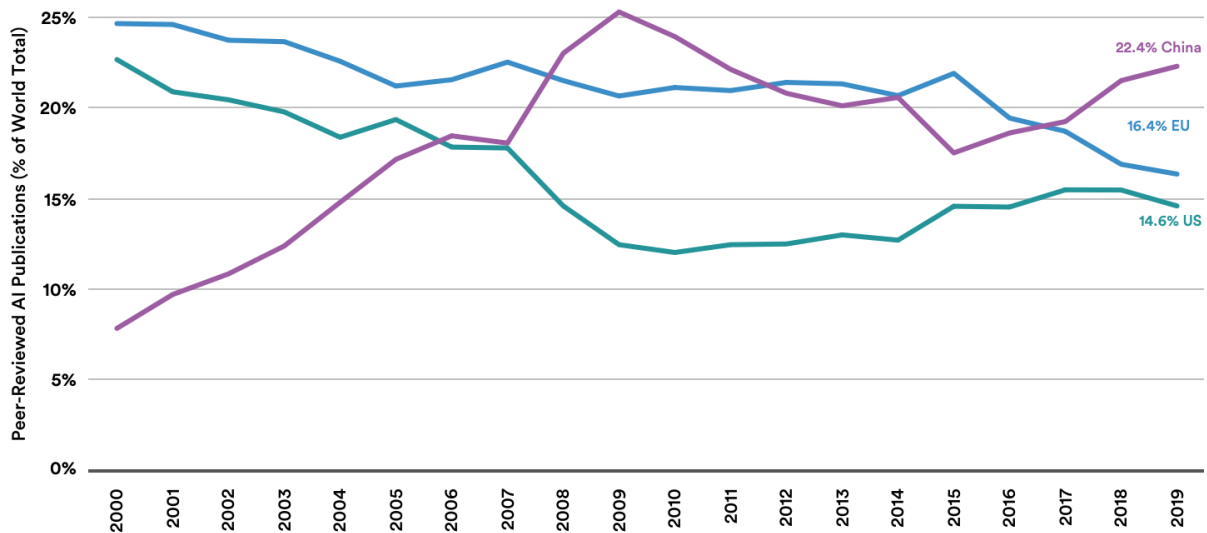


Fig 9: Peer-reviewed AI publications (% of world total) by geographic area, 2000-2019 Elsevier/Scopes, 2020 | Chart: (Zhang et al., 2021)

Academic institutions are the leaders in AI scientific publishing worldwide. However, the second source differs since affiliated corporate papers share 19.2% of total publication in the US, while the government is the second most prominent in China (15.6%) and the EU (17.2%). For 2015 - 2019, the US had the most significant number of hybrid academic-corporate, co-authored, peer-reviewed AI publications, more than double the EU's, which ranked second, followed by China in third place (Zhang et al., 2021).

Concerning digital innovation, the US is leading worldwide in terms of patent applications, and China is more prominent in data collection and data access, the primary source for developing AI technologies. According to a report published by WIPO in 2019, until early 2018, patent and scientific publication statistics indicated that the European presence in several rankings was due to Germany alone. **Starting from AI techniques, Germany was the only European country appearing in the top five states for all the examined categories (Probabilistic reasoning, Ontology engineering, Fuzzy logic, Logic programming, and Machine learning) regarding the patent filings.** Nevertheless, **for scientific publications, the scene changes, with France and Italy in the top five countries.** France stood out in Logic programming and Italy in the Ontology engineering sector. Similarly, in patenting AI functional applications, Germany was the only European country in the top five countries ranking internationally. Germany held prominent positions in publications for all the examined groups, France was fifth in Distributed AI and Knowledge representation and reasoning, and Spain fifth in Predictive analytics.

The global value of VC investments in 2020 was near to US\$ 75 billion, starting from less than US\$ 3 billion in 2012. Start-up firms established in the US and China absorbed more than 80% of investments in 2020. The EU was next with only 4% and the UK and Israel, both at 3%. Within the EU, AI firms in Germany and France absorbed two-thirds of VC investments in 2020 (Tricot, 2021). The VC significant growth is a strong sign that the AI industry is maturing, but the gap between the EU and US and China still remains (Tricot, 2021).

The top industries for AI start-ups based in the US were mobility and autonomous vehicles (30% between 2012 and 2020); healthcare (13%); business processes and support services (11%); IT infrastructure and hosting (10%); media, social platforms and marketing (8%); and financial and insurance services (7%). On the other hand, Chinese AI start-ups preferred industries were mobility and autonomous vehicles (41% of VC investments from 2012 to 2020); media, social platforms and marketing (14%); robots, sensors and IT hardware (13%); IT infrastructure and hosting (8%); and business processes and support services (7%). EU27 start-ups invested between 2012 and 2020, mainly in media, social platforms and marketing (20%); business processes and support services (19%); financial and insurance services (16%); IT infrastructure and hosting (13%); and, healthcare, drugs and biotechnology (12%) (Tricot, 2021).

4.2 Determinants of technology integration by firms at country level

4.2.1 Introduction

Accenture Research and Oxford Economics have estimated that the digital economy, involving some form of digital skills and capital, accounts for 22.5% of global GDP, while its potential is far from having been reached²⁸. Before the pandemic outbreak, digitalisation was mainly familiar to larger players, usually having adopted a technological orientation. However, the new digital circumstances and needs have created a unique opportunity for more traditional sectors to digitalise their business models. By optimising their business model, firms can significantly reduce their operational costs, provide better products and customer services, increase consumer welfare, and use data analytics to improve their performance and, generally, boost their efficiency. As a result, their productivity potential will grow, contributing to their competitiveness and sustainability.

The positive spillovers for the economy are high. **Accenture Research and Oxford Economics estimate that using an optimal combination of investments in digital skills, digital technologies, and digital accelerators could increase US GDP by 2.1%—which equates to US\$ 421 billion in 2020.** Considering the digital gap, as described extensively above, among the EU and other leading countries, such as the US and China, the Union needs to act immediately to ensure a fair share of this digital source of global growth.

To explore further the determinants of digital integration by firms, we have conducted a short exercise by utilising the data of I-DESI for the period 2015-2018. **Our objective was to stress the key factors that enable firms to optimise their technological integration fully. Our analysis does not intend to establish causality but only to find significant correlations among the different dimensions of digital advancement.** The variables included in the study are all normalised (in the interval 0 to 1). Hence, the coefficients are comparable, and we can easily distinguish the gravity of each dependent variable. For modelling, we employ the between estimator, and it is preferred to compare the average differences between individuals and, in our case, countries.

Our optimal goal is to provide a framework that describes the EU's firm digital performance in depth and demonstrates the essential characteristics or instruments that could positively influence it. We expect that Europe could turn to a leading economy in automation, AI, and other emerging digital technologies if the competitive advantages and weaknesses are timely and appropriately addressed. Furthermore, the results of this chapter can assist policy-makers in designing tailored policies to promote EU business digital transformation.

²⁸ <https://www.oxfordeconomics.com/recent-releases/digital-disruption>

4.2.2 Results

Regarding the average performance of the Integration of Digital Technology Dimension for 2015-2018, the top-ranking country is the Netherlands, followed by Iceland and Switzerland. The US is sixth in the ranking, while China in this indicator is significantly behind as it ranks in the last three positions. The country with the average performance is France (0.43), while the median country is Chile (0.41). The last five European countries include Poland (0.16), Lithuania, Romania, Greece and Italy (similar scores of 0.26 for each of the last four countries).

4.2.2.1 The impact on the integration of digital technology of firms by the other four main dimensions of I-DESI

Regressing the integration of digital technology against the others for the main dimensions of I-DESI, only the Citizen Use of Internet Indicator appeared statistically significant from the four main dimensions with a coefficient equal to 0.69. It is interesting to investigate what effect could influence the ranking if, *ceteris paribus*, a country increased its performance slightly. Increasing the Citizen Use of Internet Indicator by 0.1 points is associated with an increase in the Integration of Digital Technology by 0.069. For the country with the average performance (0.43, the performance of France), a new performance of 0.50 (equal to the performance of Japan) is created, resulting in the country jumping six places higher in the ranking. This finding is more important for countries with relatively low performance than top performers since the jump in the ranking is greater. For example, in Slovakia, with a performance equal to 0.30, the increase of 0.069 brings the country eight places higher with a performance almost equivalent to Korea.

4.2.2.2 Sub-dimensions of the I-DESI with a significant effect on the integration of technology by firms

In the dimension of connectivity, the statistically significant variables are: a) Fixed Broadband Take-Up; and b) Mobile Broadband Take-Up. If a change of 0.01 *ceteris paribus* occurs, the country with the mean performance (0.43 – France) will jump five and three places for a) and b), respectively. For countries with a relatively low performance, jumping in the ranking is greater for the first indicator. In the example of Slovakia, the increase of 0.01 brings the country 6 and 2 places higher, respectively. Comparing the two sub-dimensions, company integration of digital technology is stronger correlated with the Fixed Broadband Take-Up followed by Mobile Broadband Take-up. Fixed (wired)-broadband speed in Mbit/s also appeared statistically significant in the confidence interval of 90%.

Next, regarding digital skills, the statistically significant variables are: a) at least basic skills (word processing), b) at least basic software (coding). If a change of 0.01 *ceteris paribus* takes place, the country with the mean performance (0.43 – France) will jump five places for a), but the effect is negligible for coding. For countries with relatively low scores, the scaling in the ranking is greater. For instance, in Slovakia, the increase of 0.01 brings the country eight and one place(s) higher, respectively. Notice that the effect of basic knowledge is significantly higher.

Last but not least, if we compare the integration of digital technology by firms only with the sub-dimensions of Citizen Use of Internet, we find that fixed broadband traffic (GB/mth/person) is statistically significant. This fact implies that the increased use of the Internet positively affects a firms' motivation to digitalise. A minor change will affect countries with relatively low performance, such as Lithuania, where the increase of 0.01 brings the country four places higher. On the other hand, Luxembourg, a country with a quite increased performance, will be two positions higher.

5. Regulating the digital economy. A transatlantic perspective

5.1 The European Regulatory Framework

5.1.1 Digital sovereignty and the evolution of the European digital strategy

The last decade has been characterised by digitisation accelerated by the Covid-19 pandemic which has highlighted the importance of improving and accelerating digitisation and achieving strategic autonomy in developing digital solutions in line with the EU's founding principles and values.

If digital sovereignty has become clearly central in the European debate and initiatives launched by the European institutions, the recognition of the importance of digital and the need to make the EU a leader in this field has, however, been rooted for many years. In fact, on **6 May 2015**, the European Commission launched "**A Digital Single Market Strategy for Europe**" (DSM) to create a market in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. The DSM Strategy is built on three pillars, including 16 specific initiatives: 1) better access for consumers and businesses to online goods and services across Europe; 2) creating the right conditions for digital networks and services to flourish; 3) maximising the growth potential of our European Digital Economy.

From the adoption of this strategy, several initiatives were launched by the Commission and targets had become increasingly ambitious until the adoption, on **19 February 2020**, of the Communication "**Shaping Europe's digital future**". Its macro-objectives are the implementation of technologies at the service of individuals, the creation of a fair and competitive digital economy and the realisation of an open, democratic and sustainable society.

In her State of the Union address in September 2020, President von der Leyen announced that Europe should secure digital sovereignty with a common EU vision by 2030, based on clear goals and principles, emphasising on a European Cloud, leadership in ethical AI, a secure digital identity for all, and vastly improved data, supercomputer and connectivity infrastructures. In response, the European Council called for an intensification of the work begun in the past decade to accelerate Europe's digital transformation. This would be built on progress towards a fully functioning Digital Single Market and strengthening actions defined in the strategy for Shaping Europe's digital future, and invited the Commission to present a comprehensive Digital Compass by March 2021, setting out digital ambitions for 2030, establishing a monitoring system and outlining key milestones and the means of achieving these ambitions.

Following up on these requests, on 9 March 2021, the European Commission published the Communication "**2030 Digital Compass: the European Way for the Digital Decade**". It focuses on four main areas representing the expression of digital sovereignty dimensions already described - secure and sustainable digital infrastructures, digital transformation of businesses, digital skills of citizens and digitisation of public services. Considering that digitisation can become, especially

during the pandemic, a decisive enabler of rights and freedom, allowing people to reach out going beyond specific regions, social positions or community groups, and opening up new opportunities to learn, enjoy oneself, work, explore and fulfil one's ambitions, the strategy set out a programme of policy reform. This has already started with the Data Governance Act, the Digital Services Act, the Digital Markets Act and the Cybersecurity Strategy (to be analysed in the following paragraphs).

Specifically, on digital infrastructures, the strategy underlines the importance to ensure an excellent and secure connectivity for everybody and everywhere in Europe and achieve gigabit connectivity by 2030. To this end, any technology mix can be used even if the focus should be on the more sustainable next generation fixed, mobile and satellite connectivity, with Very High Capacity Networks including 5G being rolled out.

The document also highlights the necessity to develop microprocessors (essential for connected cars, smartphones, IoT, AI, high performance computing, edge computing) fixing a goal by 2030 - that the production of cutting-edge and sustainable semiconductors in Europe including processors will be at least 20% of the world production (meaning manufacturing capacities below 5nm nodes aiming at 2nm and 10 times more energy efficient than today). Concerning data infrastructures, considering that EU-based cloud providers hold only a small share of the cloud market and the volume of data generated is greatly increasing, the communication emphasises the necessity to strengthen its own cloud infrastructure and capacities to ensure security.

Where the digitisation of enterprises is concerned, the strategy sets high goals by 2030 and, specifically, the take up of cloud computing services, big data and AI by 75% of European enterprises, the acquisition of at least a basic level of digital intensity by more than 90% of European SMEs and the growth of the pipeline of European innovative scale ups and the improvement of their access to finance, leading to doubling the number of unicorns in Europe.

Finally, regarding the digitalisation of public services the EU's objective, by 2030, is to ensure that democratic life and public services online will be fully accessible for everyone. The strategy specifically proposes the following level of ambition - 100% online provision of key public services available for European citizens and businesses, 100% of European citizens with access to medical records (e-records) and 80% of citizens able to use a digital ID solution.

To guarantee achieving these ambitions, the communication proposes a Digital Compass in the form of a policy programme to be adopted by a European Parliament and Council co-decision, including concrete targets and an articulated governance structure²⁹. Specific attention is focused on the multi-country projects that should be able to build a common and multi-purpose pan-European interconnected data processing infrastructure and a pan-European blockchain-based infrastructure, endow the EU with capabilities in electronics design and deployment of the next generation of low power trusted processors and other electronic components, develop Pan-European 5G corridors, acquire supercomputers and quantum computers, deploy an ultra-secure quantum communication infrastructure and a network of Security Operations Centres, encourage connected public

²⁹ The model proposed provides an annual reporting by the Commission to the European Parliament and Council on the progress towards the Digital Decade, the monitoring of digital principles endorsed in the inter-institutional declaration and a mechanism to organise with Member States those Multi-Country Projects that are necessary for building Europe's digital transition in critical areas.

administrations, complete an EU-wide network of “European Digital Innovation Hubs” and establish high tech partnerships for digital skills through Pact for Skills.

5.1.2 Data regulation: from the GDPR to the Data Act

Data is the lifeblood of the digital revolution. The regulatory analysis shows a growing interest in the subject as a consequence of the rapid and important technological evolutions that have led to the appearance of new criticalities to be solved. The attention of European institutions has for years been focused on data regulation and, in particular, on personal data. Art. 8 of the Charter of Fundamental Rights states that everyone has the right to the protection of their personal data, so safeguarding the right to privacy is one of the main objectives of European institutions.

In the first phases, European institutions drew up a regulatory framework based on Directive 95/46/EC on the protection of individuals relating to the processing of personal data and on the free movement of such data, Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, Regulation (EC) No 45/2001 on the protection of individuals relating to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and Directive [2002/58/EC](#) – the E-Privacy Directive. These are the first initiatives to ensure a set of rules able to guarantee the protection of personal data in the EU.

However, the most important initiative, which has enabled the EU to become a model at global level, is the adoption, in April 2016, of **Regulation n. 2016/679** on the protection of individuals concerning the processing of personal data and on the free movement of such data. This is a very important regulatory step that has laid down the foundations of the lawfulness of data processing, clearly indicating the timing, contents and modalities of the information notice, defining the rights of data subjects (access, cancellation-oblivion, limitation of processing, objection, portability), identifying the subjective characteristics and responsibilities of data controllers and data processors (introducing, among the various criteria, that of 'data protection by default and by design' and of risk) and regulating international data transfers. One of the most important aspects concerns the territorial scope.

Later, on 23 October 2018, **Regulation n. 2018/1725 on the protection of natural persons regarding the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) n. 45/2001 and Decision n. 1247/2002/EC** was adopted. It lays down rules on how EU institutions, bodies, offices and agencies should treat the personal data they hold on individuals, upholds an individual’s fundamental rights and freedom, especially the right to protection of personal data and the right to privacy, and aligns the rules for EU institutions, bodies, offices and agencies with those of the GDPR and Directive (EU) 2016/680.

Considering the objectives set by the European Union's strategy since 2015, but also the technological developments that have emerged on the market (new Internet-based interpersonal

communication services or new IoT technologies), on 10 January 2017, the European Commission launched a proposal for a **regulation concerning the respect for private life and the protection of personal data in electronic communications, repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)**. In detail, the proposal, which is the subject of a complex adoption procedure that has not yet been finalised, aims to ensure a higher level of privacy protection for users of electronic communications services, consistent with the GDPR and the state of the art. It establishes rules on the protection of fundamental rights and freedom of natural and legal persons related to the provision and use of electronic communications services, primarily the right to privacy and communications, and the protection of individuals for the processing of personal data. This proposal, in particular, starting from the consideration that electronic communications data must be confidential, identifies permitted processing of electronic communications data, regulates storage and erasure of electronic communications data and consent (in line with the GDPR), prescribes information and options for privacy setting, and sets specific rules on incoming call blocking, publicly available directories and unsolicited communications fixing information obligations on providers specifically concerning the consent of end-users.

Alongside the need to ensure the effective protection of personal data, the intention of the institutions to ensure that individuals, businesses and public administrations can benefit from the enormous opportunities associated with the use of data is also a priority. As digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans and data is at the heart of this transformation, on 14 November 2018, **Regulation n. 2018/1807 on a framework for the free flow of non-personal data in the European Union** was adopted. It aims at ensuring the free flow of data, other than personal data, within the Union by laying down rules on data localisation requirements, the availability of data to competent authorities and the porting of data for professional users. To this end, the regulation encourages the development of self-regulatory codes of conduct at EU level in order to contribute to a competitive data economy, based on the principles of transparency and interoperability, and taking due account of open standards (to be developed in close cooperation with all relevant stakeholders, including associations of SMEs and start-ups, users and cloud service providers) and prescribes MSs to designate a single point of contact for the application of this regulation.

Successively, focusing on the public sector, the European institutions adopted **Directive n. 2019/1024 on open data and the re-use of public sector information (Open Data Directive)** which sets timelines, procedures to process the request for re-use and the conditions for re-use identifying available formats and principles governing charging and conditions (specific rules are set for high-value datasets). The same directive encourages MSs to make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine readable format and portal sites that are linked to the asset lists, and support the availability of research data by adopting national policies and relevant actions to make publicly funded research data openly available.

In February 2020, the Communication “*A European Strategy for Data*” outlined the European strategy consisting of a series of measures and investments to enable the data economy over the next five years. This communication fully presents a European data strategy aimed at making the EU the most attractive, secure and dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all of its citizens. To achieve this goal, the document identifies several critical issues that need to be overcome concerning the availability of data, imbalances in market power, data interoperability and quality, data governance, data infrastructures and technologies, empowering individuals to exercise their rights, skills and data literacy and cybersecurity. Considering these issues, the Commission has outlined a strategy focused on four pillars and several key actions to encourage a cross-sectoral governance framework for data access and use, to strengthen Europe’s capabilities and infrastructures for hosting, processing and using data, interoperability to reinforce competences and skills and to create common European data spaces in strategic sectors and domains of public interest (specifically, manufacturing, the Green Deal, Mobility, Health, Finance, Energy, Agriculture, Public Administrations and Skills).

In implementing the strategy, on 25 November 2020, the Commission proposed a regulation on European data governance (**Data Governance Act**). This proposal is the first deliverable under the European Strategy for Data and aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The proposal, complementing Directive n. 2019/1024 of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive), includes measures to: 1) increase trust in data sharing, as the lack of trust is currently a major obstacle and results in high costs; 2) create new EU rules on neutrality to allow novel data intermediaries to function as trustworthy organisers of data sharing; 3) facilitate the reuse of certain data held by the public sector; 4) give Europeans control over the use of the data they generate, by making it easier and safer for companies and individuals to voluntarily make their data available for the wider common good under clear conditions.

The regulation lays down conditions for the re-use, within the Union, of certain categories of data held by public sector bodies, identifies specific data sharing services subject to notification procedure to the competent authority (which may charge fees) and identifies the information to be included, regulates data altruism and general requirements for registration of data altruism organisations, identifies requirements relating to competent authorities and sets the right to an effective judicial remedy. Moreover, it allows the Commission to establish a European Data Innovation Board in the form of an Expert Group, made up of representatives from competent authorities of all the MSs, the European Data Protection Board, the Commission, relevant data spaces and other representatives of competent authorities in specific sectors, and identifies the tasks.

More proposals on data spaces are expected to follow in 2022, complemented by a Data Act to foster data sharing amongst businesses, and between businesses and governments.

One of the most important themes of the European strategy concerns the enabling technologies and, in particular, **cloud services**. Starting from the consideration that the most important cloud service providers are non-EU companies, the Commission is mainly concerned about the issues regarding data ownership and management within European MSs and on the potential lack of privacy and absence of data protection for personal information collected by foreign providers.

Faced with the several MS attempts to develop national strategies, possibly conflicting *de facto* with the principles of a single digital market, the European Commission has recently proposed the creation of a European cloud initiative within the second pillar of the strategy "A European Strategy for Data". Therefore, the Commission is promoting the setting up of the "Gaia-X" cloud project, a federated data infrastructure to enable the management, access and control of data belonging to EU citizens and businesses. The aim of the initiative, launched by France and Germany, is to ensure interoperability and security standards in order to promote an open and transparent digital ecosystem, where data and services can be made available and collected and shared in a secure environment, rather than creating a European cloud alternative to the US and Asian providers. The project envisages the creation of a new pan-European platform that brings together different cloud service providers, including non-Europeans, as long as they accept the set of requirements, standards and values promoted at EU level, and above all data sovereignty for users.

In addition to the commitment to setting up the European federal cloud within the framework of the Gaia X project, on December 2020, the European Commission launched a **European Alliance on Industrial Data, Edge and Cloud**, made up of MS representatives from MSs, cloud computing providers and industrial cloud users. It will feature the development of several work streams, related to key EU policy goals: 1) joint Investment in cross-border cloud infrastructures and services to build the next generation cloud supply, including enabling Common European Data Spaces; 2) a EU Cloud Rulebook for cloud services providing a single European framework of rules, transparency on their compliance and best practices for cloud use in Europe; 3) a European marketplace for cloud services where users will have a single portal to cloud services meeting key EU standards and rules. It is expected to lead the implementation of the pan-European cloud with a budget of up to € ten billion.

5.1.3 The EU legal framework on Artificial Intelligence: from the Communication "AI for Europe" to the AI Act proposal

AI is expected to revolutionise many if not all aspects of our social and economic life, create new business opportunities and improve people's daily activities. The potential of this technology is expected to affect not only the industrial field, but also private life and the public sector.

The start of EU's pro-active approach towards AI can be set on 25 April 2018, when the European Commission presented the Communication "**AI for Europe**", the starting point of the pro-active approach towards AI within the EU. The new approach was based on three main pillars - placing the EU at the cutting-edge of technological developments, preparing EU for socio-economic changes brought about by AI and ensuring an appropriate ethical and legal framework.

Following, in June 2018, the EC announced the High-Level Expert Group on Artificial Intelligence (AI HLEG) to support the implementation of the EU Communication on AI published in April 2018 and make recommendations on how to address mid-and long-term challenges and opportunities related to AI. In the same month, the EC also launched the AI Alliance, a multi-stakeholder forum to provide feedback to the AI HLEG. Moreover, the Coordinated Plan on AI, published on 7 December 2018, required MSs to adopt AI strategies, including budget figures, to be possibly and considerably increased in the following years.

In April 2019, the AI HLEG presented the “*Ethics Guidelines for Trustworthy AI*” which offers guidance to all stakeholders and sets a framework for achieving trustworthy AI, identifying a list of ethical principles and providing guidance on how to translate such principles into socio-technical systems³⁰.

Moving on, in February 2020, the Commission published its White Paper, “*Artificial Intelligence: a European Approach to excellence and trust*”, paving the way for the AI package, delivered in April 2021, consisting of a Communication on Fostering a European Approach to Artificial Intelligence, the Coordinated Plan with Member States: 2021 Update, and a proposal for an AI Regulation laying down harmonised rules for the EU (**Artificial Intelligence Act**).

In detail, the AI Act establishes a list of certain prohibited practices for all AI systems as violating EU values and fundamental rights. The regulation follows a risk-based approach, differentiating between uses of AI that create an unacceptable risk, a high risk, and low or minimal risk³¹.

The regulation requires the establishment, maintenance and demonstration of a risk management system that is the result of a process of constant and systematic updating throughout the life cycle of the system, the adoption of appropriate risk management measures to be taken according to a set of criteria and principles set out in detail and following specific tests aimed at measuring their appropriateness, the preparation and preservation of supporting technical documentation, a design aimed at ensuring an adequate level of accuracy, robustness and cybersecurity, post-market monitoring obligations and reporting of serious incidents or malfunctions, and guarantees of cooperation with the competent authorities. Specific obligations are placed on importers and distributors of high-risk IA systems.

The proposed regulation takes care to define obligations also for **users** of high-risk AI systems, requiring, in particular, the use of such systems in accordance with the instructions for use, ensuring that input data is relevant to the purpose of the AI system, and the retention of logs automatically

³⁰ According to the guidelines, trustworthy AI should be: (a) lawful, complying with all applicable laws and regulations; (b) ethical, ensuring adherence to ethical principles and values; and (c) robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.

³¹ The regulation prohibits those practices considered unacceptable because they are contrary to EU values. For example, because they violate fundamental rights (e.g. manipulative practices of minors or the disabled, or that envisage the use of subliminal techniques that exploit the unawareness of individuals, etc.). In the case of high-risk AI systems, the regulation distinguishes between the main types of systems that fall into this category (AI systems intended for use as security components of products subject to ex ante third-party conformity assessment and other stand-alone AI systems that have implications primarily regarding the fundamental rights explicitly listed in Annex III), identifies the criteria to be followed in assessing whether an IA system presents high risks and lays down a series of mandatory requirements, as well as making access to the European market for such systems subject to ex ante conformity assessment, the procedures for obtaining the CE conformity marking being governed in detail by the regulation.

generated by high-risk AI systems, if such logs are under their control, for a period appropriate to the intended purpose of the AI system.

Specific transparency requirements are laid down with regard to AI systems intended to interact with natural persons, emotion recognition or biometric categorisation systems and systems generating or manipulating images or audio or video content where it is necessary to ensure that users are aware.

In addition to the obligations imposed on the development, distribution and use of AI systems, the AI Act contains several measures aimed at supporting innovation in this sector. The regulation, in fact, encourages the competent national authorities to create regulatory sandboxes and establishes a basic framework in terms of governance, supervision and responsibility, as well as measures to reduce the burden on SMEs and start-ups.

The same proposal defines **governance model**³², encourages the adoption of **Codes of Conduct**³³ and sets up a set of **penalties**.

This Commission proposal has also sparked off a wide debate at international level. Although there is broad support for the decision to establish a harmonised AI framework and to adhere to a risk-based approach focused on protecting the rights and interests of individuals, requests have been made for clarification on the content of certain obligations, for greater attention on the possible applications and uses of AI technologies rather than on the technologies themselves, and for an assessment of the scale of the costs involved, especially for SMEs and start-ups, and the potential obstacles to competition and innovation that they could represent.

5.1.4 Platforms' role and responsibility: from Directive 2000/31/CE to the DSA and DMA proposals

The last twenty years have been characterised by the growing emergence of digital services and platforms which have accompanied and facilitated the transfer of many socio-economic activities into the network, increasing market efficiency, facilitating trade and innovation and providing enormous benefits to citizens, businesses and public administrations.

The growth of platforms and the acquisition of a key central role - especially in the last two years where the services offered have made it possible to exercise fundamental rights such as the right to education - has been accompanied by radical changes in the regulatory framework. If in the early

³² In detail, the proposed regulation establishes a European Committee for Artificial Intelligence made up of the national supervisory authorities, represented by the head of the authority or by a senior official of equivalent level, and the European Data Protection Supervisor and chaired by the Commission. Its task is to gather and share knowledge and best practices among the MSs and contribute to the uniformity of administrative practices in the MSs, formulating opinions, recommendations or written contributions on questions about the implementation of the regulation. It is up to each Member State to designate a competent authority to ensure the regulation's application and implementation (also to provide guidance and advice on the regulation's implementation) and to draw up an annual report to be sent to the Commission.

³³ These Codes of Conduct should be drawn up by individual suppliers of AI systems or by organisations representing them, or by both, also with the participation of users and all other stakeholders and their representative organisations, to encourage the voluntary application to AI systems of the requirements relating, for example, to environmental sustainability, accessibility for persons with disabilities, etc.

stages, the European institutions chose to implement a system of a few rules contained in directives creating an ecosystem that, in the last twenty years, has favoured technological evolution and the proliferation of new and extraordinarily flourishing business models, the latest initiatives have put forward regulations containing specific obligations and prohibitions aimed at offering responses to new critical issues, and ensuring maximum harmonisation and legal certainty within the EU.

Directive n. 2000/31/EC has fixed few rules requiring Member States to provide for information obligations covering all the data necessary to ensure that the provider can be easily identified by the recipients of the services and by the authorities, has set specific rules on commercial communications to ensure a clear indication that the communication is a commercial communication, the clarification of the natural or legal person on whose behalf the commercial communication is made and a clear and unambiguous identification of the promotional offers. The same directive also regulates the liability regime of intermediaries and, in particular, the cases of exclusion of liability by subdividing mere conduit, caching and hosting services.

Later, on 25 May 2016, after the assessment of the role of platforms, including in the sharing economy and of online intermediaries established in the application of the DSM strategy (2015), the Communication *“Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe”*, identified the guiding policy principles to create and maintain a level playing field for comparable digital services, ensuring responsible behaviour of online platforms to protect core values, fostering trust, transparency and ensure fairness and keeping markets open and non-discriminatory to foster a data-driven economy.

The growing centrality of platforms - and connected critical issues in their relationship with business users and indirectly with consumers - has led European institutions to adopt **Regulation n. 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (better known as P2B regulation)**. The purpose of this regulation is to ensure that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities. To this end, the regulation fixes terms and conditions setting specific information obligations in favour of business users, imposes and prohibits specific contractual terms, regulates cases of restriction, suspension and termination online intermediation services, prescribes disclosure obligations on the main parameters determining ranking and the reasons for the relative importance of those main parameters as opposed to other parameters, identifies the content of differentiated treatment description, and regulates access to data and mediation procedures. Additional consumer protection is provided by **Directive n. 2019/2061 (Enforcement and Modernisation Directive)**.

Directive n. 2018/1808 (AVMS Directive) marks a further regulatory development to regulate online platform operations. For the first time, the AVMS Directive has extended some of the rules of the audiovisual sector also to video-sharing platforms and to audiovisual content shared on the social media (if the provision of user-generated programmes and videos is an essential feature). The directive has laid down specific obligations on these entities to protect minors, invest in European works and respect advertising limits.

The new leadership of the European Commission took office at the end of 2019, immediately showing its willingness to go further towards a more stringent regulation. The guidelines for the period 2019-2024, published at the end of January, and the digital strategy outlined in the Communication “Shaping Europe's digital future” of 19 February, clearly revealed the Commission's desire to address the new opportunities and critical issues related to digitisation and the new role played by platforms by defining new rules for digital services.

Consequently, on 15 December 2020, the European Commission published a package of two legislative initiatives - the **Digital Services Act (DSA)** and the **Digital Markets Act (DMA)**. In order to promote maximum harmonisation within the EU and thus overcome the current regulatory fragmentation, the Commission has opted for two proposals for regulations containing specific obligations and prohibitions.

The DSA proposal, specifically, published after the conclusion of a public consultation - launched on 2 June 2020 and ended on 8 September -, is divided into **five chapters** which introduced a horizontal framework for all categories of content, products, services and activities on intermediation services in which, however, a **diversified liability regime** is outlined based on the services offered and the size of the supplier (e.g. some obligations are limited only to very large online platforms, which have acquired a central and systemic role due to their scope)³⁴.

³⁴ The proposal, after reiterating the distinction between mere conduit, caching and hosting services and regulating exemptions from liability, imposes different due diligence requirements. Specifically, the regulation requires all providers of intermediation services, regardless of size and the service offered, to establish a single point of contact for direct communication with the state authorities, the identification, for providers not established in the EU, of a legal representative in one of the MSs in which it offers its services, the inclusion in clear and accessible language in its terms and conditions of information concerning any restrictions imposed on the use of the service, including those relating to policies, procedures, measures and tools used for the moderation of content, including the algorithmic decision-making process employed and the publication, at least once a year, of reports (ex. art. 13), easily understandable and detailed on any moderation of content undertaken by them in the reference period (with specific information including the number of measures received by the authorities of the MSs, divided on the basis of the type of illegal content they relate to, with an indication of the average time required to take the required action).

In addition to the above, the proposal introduces specific provisions for certain types of providers. Concerning, in particular, providers of hosting services, including online platforms, the regulation provides for the establishment of notification and action mechanisms that allow individuals and entities to report the presence of illegal content, providing information (including the precise indication of the URL or URLs) on which the same provisions configure precise obligations of feedback (also defining the information to be transmitted in the feedback) and the sending of a detailed and reasoned information to the recipients of the service about the decision to remove or disable access to certain information (the decisions taken and the relative supporting reasons to be published in a public database managed by the Commission).

With regard to online platforms (with the exclusion of platforms qualified as micro or small enterprises), the proposed regulation prescribes the provision of an internal system for handling complaints against decisions to remove or disable access to information, suspend or interrupt the provision of the service, in whole or in part, to recipients, and suspend or close the recipients' account, the possibility for the recipients of the service to appeal an out-of-court dispute resolution body, the provision of technical and organisational measures to ensure that warnings coming from "trusted reporters" are processed and decided on a priority basis, the provision of measures and protection against abuse, specific provisions for the notification of suspected offences, the traceability of sellers and the respect of transparency obligations specifically in online advertising.

Additional obligations are imposed on large platforms identified as counting on at least 10% of the EU population (45 million users), which are required to carry out an annual risk assessment, undergo, at its own expense, an audit at least once a year by an independent organisation, maintain and make public (for at least one year from the last time the advertisement was displayed) a file containing information relating to the content, applicant and recipients of the advertisement and the period during which the advertisement was displayed. It must also allow the Commission and the Coordinator access to the data, following a specific request

The same proposal places **specific obligations on the Member States** to verify the compliance of these subjects operating in their respective territories with respect to the provisions contained in the proposed regulation, also establishing new subjects (Coordinators for Digital Services) and defining mechanisms of enforcement and cooperation among states.

The proposal also encourages the development of **Codes of Conduct** that set objectives to be pursued, identify performance indicators in relation to the achievement of these objectives - which the Board, in bringing together the Coordinators, will monitor - and take into account the interests of all EU stakeholders, including citizens. The adoption of Codes of Conduct is also encouraged for online advertising in order to ensure adequate protection of the rights of all stakeholders and the establishment of a competitive, transparent and fair environment for online advertising.

In defining the **structure of governance**, the proposed regulation imposes on Member States to identify **one or more authorities responsible for the regulation's application** and of a **Coordinator for the Digital Services** and institutes the European Board for the Digital Services.

The same regulation also describes the **cooperation procedures** among the Coordinators, regulates the modalities through which joint investigations can be carried out and provides for the possibility of activating the **investigative and enforcement powers of the Commission** in the case of suspicion of regulation violation by the large platforms. The regulation establishes the criterion to be followed to identify the **jurisdiction**, connecting it to the MS where the supplier's head office is located, while for suppliers not established in EU, the state where the legal representative is established will have jurisdiction.

In order to ensure compliance with the provisions of the regulation, the proposal provides for the possibility for MSs to provide for **penalties** of up to 6% of the supplier's annual turnover (1% in the case of non-compliance, e.g. failure to submit to inspection, failure to respond to requests for information, etc.).

The DSA proposal will bring about important changes, redesigning the role and responsibilities of platforms and producing a strong impact on them. The new proposed regulatory framework has triggered a wide debate among stakeholders. On the one hand, there is a call, especially by the MSs, to better clarify the mechanisms for cooperation and coordination with the Commission in order to ensure effective action. On the other hand, instead, there have been requests to rethink the type of obligations imposed on suppliers in view of their practicability and sustainability and in consideration of the impact on security and specific business models, to strengthen regulatory dialogue to customise obligations and sanctions, to extend some obligations, especially those for the protection of consumers, also to SMEs, to strengthen and extend certain requirements on online advertising, to reinforce the obligation to trace traders by extending the scope of certain provisions to all intermediary services and by introducing new provisions aimed at online markets, to set

and for a reasonable period of time indicated in the same request, identify its own compliance officers, transmit, in addition to the reports foreseen for the other suppliers, to the Commission and the Coordinator, a report containing the risk assessment and the relative risk mitigation measures, the audit report and the report on the implementation of the measures requested during the audit.

stricter deadlines for taking action on high-impact content and to clarify the concept of illegal content in order not to undermine the harmonisation efforts of the proposed framework.

The **DMA proposal**, instead, is aimed at those platforms that increasingly act as gateways or gatekeepers between commercial users and end users, hold an established and long-lasting position and the power to make improper use of user data, reinforce barriers to market entry and engage in misconduct towards commercial users and end users. The scope of this regulation is focused on "core platform services", that is, online brokerage services, online search engines, social networks, video sharing platforms, number-independent interpersonal communication services, operating systems, cloud computing services and advertising services, including any advertising networks, advertising exchanges and any other advertising brokerage services, provided by a provider of any of the above services.

For the purposes of defining the prerequisites for qualifying a provider as a gatekeeper, the proposed regulation requires (art. 3) specific conditions³⁵ and prescribes that the possession of these requirements determines the provider's obligation to notify the Commission, although the Commission has the power, independently, to identify as a gatekeeper the provider who fails to comply with this notification obligation. In addition, the Commission would have the power to review the gatekeeper status of a particular ISP in the event of a material change in the basis for the gatekeeper decision, or if the gatekeeper decision was based on incomplete, incorrect or untrue information. In general, the proposed regulation requires the Commission to verify, at least every two years, whether gatekeepers are meeting the requirements of the regulation and whether additional providers are meeting those requirements.

³⁵ In particular, the proposal requires: 1) a significant impact on the internal market, which is presumed whenever the undertaking has an annual turnover in the European Economic Area of at least € 6.5 billion during the last three financial years (or where the average market capitalisation was at least € 65 billion during the last financial year) and offers the service in at least three MSs; 2) an important gateway to reach end-users, which occurs when the provider connects a large user base to a large number of businesses (specifically more than 45 million monthly active end-users established or located in the Union and more than 10,000 active business users per year established in the Union in the last financial year); 3) possession (or foreseeable possession in the near future) of an entrenched and durable position in its operations. This requirement is deemed to be met when the thresholds referred to in point b) have been reached in each of the last three financial years.

The same proposal sets several obligations³⁶ and prohibitions³⁷ on gatekeepers and introduces the possibility to exceptionally suspend in whole or in part, a specific obligation - adopting a specific decision at the latest 3 months following receipt of a complete reasoned request - where the gatekeeper demonstrates that compliance with that specific obligation would endanger, due to exceptional circumstances beyond the control of the gatekeeper, the economic viability of the operation of the gatekeeper in the Union, and only to the extent necessary to address such threat to its viability (art. 8).

Aware of the speed of technological change, the Commission provides the possibility to conduct a **market investigation** with the purpose of examining whether one or more services within the digital sector should be added to the list of core platform services or to detect types of practices that may limit the contestability of core platform services or may be unfair and which are not effectively addressed by this proposal.

The proposed regulation defines in detail the **powers of the Commission**, granting it the power to request information, conduct inspections, order interim measures, make binding commitments proposed by the gatekeeper, carry out monitoring activities regarding compliance with the obligations under the proposed regulation, adopt decisions certifying infringements by gatekeepers and impose **penalties**. The latter, in particular, are quantified up to 10% of the total annual worldwide turnover of the company. Moreover, systematic violation of the regulations may lead to the application of extraordinary **structural remedies** such as the obligation to sell part of the company's assets or property (splitting).

In carrying out the activities regulated in the DMA, the Commission is assisted by the Digital Markets Advisory Committee.

Commission decisions and sanctions imposed by the Commission are subject to the jurisdiction of the EU Court of Justice, which may cancel, reduce or increase them.

This proposal is also triggering a wide-ranging debate among stakeholders and between Member States and the Commission on the general framework as well as on the governance.

³⁶ The art. 5 prescribes gatekeepers to:

- a) allow third parties to inter-operate with the gatekeeper's own services in certain specific situations;
- b) allow their business users to access the data that they generate in their use of the gatekeeper's platform;
- c) provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements hosted by the gatekeeper;
- d) allow their business users to promote their offer and conclude contracts with their customers outside the gatekeeper's platform;
- e) ensure the effective portability of data generated through end-user or business activity.

The proposal also sets a broad obligation on gatekeepers to inform the Commission of "any intended concentration involving another provider of core platform services or of any other services provided in the digital sector" (art. 12), and the submission to the Commission, within six months of their designation as gatekeepers, of a description, verified by an independent party, of all consumer profiling techniques that the gatekeeper applies to or through its services (art. 13).

³⁷ Gatekeepers will be prohibited to:

- a) treat the services and products offered by the gatekeeper itself more favorably than similar services or products offered by third parties on the gatekeeper's platform;
- b) forbid consumers from connecting with businesses hosted outside of gatekeeper platforms;
- c) prevent users from uninstalling any pre-installed software or applications if they so desire;
- d) use business users' data for the purpose of competing with them.

In fact, although there is a wide consensus about the need to rethink the current set of rules to provide answers and remedies to the existing competitive issues, there are doubts about the capacity of a regulatory system based on an ex ante logic and strict rules to be future proof in a sector with a very high speed of innovation, as is the choice of laying down uniform rules for entities with markedly different business models and organisations (though this need is countered, at least in part, by the goal to guarantee certainty, predictability and uniformity). To this should be added the need to ensure that the quite pervasive powers granted to the Commission are mitigated and corrected by the establishment of a regulatory dialogue, with precise deadlines not delaying the Commission's speed of intervention, ensuring adequate weighting of the individual situation being analysed. Moreover, in order to achieve an effective enforcement, the right balance between a centralised framework, led by the Commission, and an active involvement and support of the MSs and their competition and regulatory authorities, has to be struck.

5.1.5 Limits and potential drawbacks of the EU regulatory approach

Notwithstanding the widespread complacency in EU policy-making circles on the so-called “Brussels effect” (Bradford, 2020), Europe is lagging well behind the US and East Asia in digital competitiveness. Lack of investment and its fragmentation across Europe could be singled out as the main culprits, but it is also time to assess if the regulation is contributing positively or negatively to this dire situation. Protecting fundamental rights is not in question, but excessive regulatory burdens could stifle innovation, slow down digital adoption, obstruct start-ups from scaling up, and disproportionately punish risks being taken by innovators. Moreover, internal market fragmentation renders the Brussels effect as mostly an illusion, at least from a European perspective. For a EU-based start-up, selling goods or services in other MSs still involves costs and organisational structures that many cannot afford, independently from how innovative they may be. By overly focusing on the Brussels effect, without solving the issues that regulation leaves unchanged or sometimes exacerbates on the internal front, could be a satisfying power play for some, but it can also give rise to existential risks for the European digital sector and, ultimately, for EU digital sovereignty.

Therefore, initiatives such as the AI Act, the Digital Strategy, the DMA and the DSA are highly fit for the need for a stronger single digital market, that could leave behind the current risks (and the increasing reality) of regulatory fragmentation. However, the new regulatory framework, if needed to face the new challenges, must also deal with the concrete possibility of unintended consequences that could stifle innovation and, paradoxically, competition.

Digital markets display high rates of dynamism and innovation, with market dynamics having shown an increasing rate of speed in the introduction and spreading of new services. We have witnessed sudden and radical shifts in the composition of market share, which continuously highlight the level of competitiveness digital platforms are exposed to, confirming a fair degree of scalability of many

of these sectors. To quote some data, Instagram took six years from its launch to gain the same amount of monthly active users that TikTok managed to achieve in less than three years, while Facebook took more than four.

The relationship between innovation and competition is extremely complex, even more so in digital markets where new technologies risk becoming obsolete and outdated within a few years. Therefore, over-regulation could be harmful both in terms of technological development and competition on price, variety and efficiency.

From a more general point of view, various types of Internet sectors show a high degree of flexibility which makes the composition of market share vary according to different geographical macro-areas. In the case of e-commerce, for instance, new local-based large marketplace operators are emerging in Europe, Latin America and especially in Asia, where players like Amazon have not yet reached a 1% market share.

As for the segmentation identified by the DMA, it is worth noting that it is extremely complex to identify clear boundaries and distinctions, for instance, between video-sharing services like YouTube and social networks like TikTok. Indeed, there are now numerous cross-sector platforms, which are continuously seeking to expand their range of possibilities and services and aim at increasing user-friendliness and opportunities, as well as customising their services to meet new trends or consumer preferences.

The same can be said for the advertising market, which has become very complex to analyse as different “channels” and formats are now not only converging, but also creating different subsectors in which players from different environments compete with each other for consumer attention. Converging technologies and strong competition for consumer attention has increasingly blurred the boundaries, so that, for instance, both the social media (such as Facebook and TikTok) and video sharing platforms (such as YouTube), as well as potentially personal communication tools such as WhatsApp, compete for video consumption on different formats and devices, making it extremely challenging to define the relevant markets.

This is also true for searches. Even if the global market structure is very concentrated, technological trends continuously challenge the incumbent, such as the spread of non-conventional search methods - voice search technologies, the use of social media platforms for commercial information searches, and the use of image recognition tools on mobile devices. The market is shifting from desktop to mobile services, making future developments harder to predict. The channels used are multiple, and involve searches, social media, banners, videos and other means in a mix that appears to be rather unclear at the moment.

Moreover, the DMA would limit a competitive channel playing an increasingly prominent role in digital markets. According to the theory of “mologopoly” (Petit, 2020), large tech companies coexist both as monopolies and oligopolies that compete against each other, bringing significant benefits to consumers under extensive circumstances. Ruling out this possibility or restricting it too much could damage both competition and innovation. The same could be true for the so-called “killer acquisitions”, negatively affecting venture capital and start-up growth.

At the same time, for instance in areas such as AI, it would be a mistake if the EU overly relies on regulation in order to establish itself as a global leader in the field. That chance would never come about unless the Old Continent achieves a leading role in the development of AI technologies. While the focus on protecting human rights in the digital field is extremely important, it should be noted that the EU is slowly falling behind in AI development when compared to other countries, such as China, the US and even the UK. What European institutions need to take into consideration is that if the race in AI development accelerates and the gap between the EU and the other countries becomes even wider, this will most certainly affect the chances for the EU to establish itself as a leading force in the regulatory framework for AI. Therefore, significant and well targeted investments need to accompany any regulation. Otherwise, an effective regulation would never be achieved.

5.2 The Regulatory Framework in the US

5.2.1 The US approach to regulating the digital field

Developments in digital technologies are increasingly shaping the global economy, and the changes brought about by these developments are affecting almost all industries, from new to traditional sectors. As economies become more digitalised and more reliant on both Internet-based networks and digital sales, governments have been increasingly called on to regulate the digital field. Nevertheless, the approaches that have been adopted for the regulation of the digital economy differ from case to case. One of the major players in this field, the United States, has been strongly conditioned in its regulatory approach by the overall vision of an essentially self-regulating market. When applying this approach to the digital field, the core idea is that the digital industry should lead the regulation of the Internet itself, thus leaving more space for actors and technical bodies, requiring the active intervention of national government to a lesser degree. This approach differs from the one chosen by another important player, the European Union. Over the last decades, the EU has opted for a more proactive role and gradually developed a consistent regulatory framework in the digital area. With this different approach, the EU has gradually established its regulatory influence in the global arena and now plays a crucial role in shaping digital markets. While the EU has worked assiduously to clearly regulate several aspects concerning consumer protection in these rapidly evolving markets, the US has instead taken a more “laissez-faire” approach on topics such as privacy, copyright, and the movement of personal and business data (Burwell, 2018). Nevertheless, as US digital platforms are being increasingly compelled to comply with European rules, it has been observed that the US has started to reverse its long-standing neutral approach and is now moving towards a more active government role in the regulation of the field.

5.2.2 Net Neutrality in the US

Network neutrality, also commonly referred to as net neutrality, is the principle according to which Internet service providers (ISPs) should treat all Internet communications equally. The principle of net neutrality implies that ISPs should not charge differently nor discriminate in other ways among websites, users, contents, platform, applications, source address, type of equipment, method of communication or destination address³⁸.

While in other western jurisdictions the principle discussed has been accepted and ultimately become part of the regulatory framework, in the US, net neutrality has been at the centre of an active debate between network users and service providers since the 1990s. The crucial issue in the conflict over net neutrality regards how the Federal Communications Commission (FCC) classifies Internet services under the Communications Act of 1934³⁹. According to the latter, if Internet services were treated as a Title II "common carrier service" the FCC would be able to strongly regulate ISPs, while if Internet services fell under Title I "information services" ISPs would be mostly unrestricted by the FCC⁴⁰.

While the Internet had already become available for commercial use in the late 1980s, back then public access was quite limited and mostly reached through dial-up modems. It was only later, between the late 1990s and early 2000s, that the Internet became more common in households and more commonly used by society, and it was during these years that the debate around net neutrality became more active. The **Communications Act of 1934 was amended in 1996 by the Telecommunications Act**, which defined the Internet as a broadcast service. The law's aim was to promote competition in the field, encourage the spread of new telecommunication technologies and reduce regulation. In 2002, the FCC established that, under the Acts of 1934 and 1996, cable Internet fell under the category of information services and, therefore, outside FCC's jurisdiction, while the Internet connection through the dial-up modem fell under the telecommunications services.

Starting from the mid-2000s, the widespread use of the Internet led to a change in the FCC approach concerning network neutrality principles. After Tim Wu came up with the theory of "net neutrality" in 2003,⁴¹ as an extension of the long-standing concept of a "common carrier", the FCC announced in 2004 a set of non-discrimination principles, called the **principles of "Network Freedom"**. These principles encouraged ISPs to guarantee users the following rights: freedom to access content,

³⁸ Easley, R., Guo, H., Kramer, J., *From Net Neutrality to Data Neutrality*, Information Systems Research, 29,2.

³⁹ Communications Act of 1934, 47 U.S.C. (1982 and Supp. V 1987).

⁴⁰ In 1966, after carrying out of a series of three Computer Inquiries, the FCC, established the distinction between telecommunications services (involving only the transmission of data) and information services (the data is processed), which are subject to different regulations, by Title II and Title I of the Communications Act, respectively, and, at the same time, fall under the authority of two different national authorities - the FCC and the FTC.

⁴¹ Tim Wu, *Network Neutrality, Broadband Discrimination*, Journal of Telecommunications and High Technology Law, Vol. 2, p. 141 (2003).

freedom to run applications, freedom to connect devices, freedom to get information about their service plan. In 2005, the Supreme Court ruled in favour of the FCC's decision, stating that even though no previous law had defined the status of cable Internet as information services, FCC had the authority to do so according to law. Following this decision, the FCC also classified Internet access via telephone lines, such as DSL, as a service of information⁴².

In 2008, the FCC ruled that Comcast had illegally hindered users from using file-sharing software as it affected the bandwidth of certain customers for video files. The FCC did not impose a fine, but ordered Comcast to cease this practice, disclosing within thirty days its network management practices and presenting how the company was planning to end the offending practices and intended future practices. A few years later, in 2010, the FCC passed the **Open Internet Order**, which forbade providers of cable television and telephone services from preventing access to competitors or certain websites. It also adopted six principles on net neutrality - transparency, no blocking, level playing field, network management, mobile and vigilance. It is worth noting that all attempts to pass bills containing net neutrality provisions in the US Congress in the period between 2005 and 2012, failed. In 2014, the DC Circuit Court determined that the FCC did not have the authority to enforce network neutrality principles if service providers were not identified as "common carriers"⁴³. After this ruling, an active public debate arose around the issue of net neutrality and whether it could be guaranteed under the existing legislation, or if it was necessary to reclassify ISPs in order to do so. On the 10 September 2014, several websites and social media participated in the "Internet slowdown" as a form of protest. In 2015, the FCC voted in favor of classifying broadband Internet services as common carriers, subjecting them to **Title II of the Communications Act, Section 706 of the Telecommunications Act**, and granting the FCC clear authority to enforce net neutrality.

However, after the appointment of its new chairperson in 2017, the FCC reversed its approach in favour of net neutrality, proposing to return to the previous classification of ISPs as Title I services, repealing neutrality policies. The main argument was that the Title II Order (on net neutrality) pushed the major telecommunications companies to reduce their capital investment in new infrastructures, thereby threatening the future of the sector. After this decision, several states, websites and platforms challenged this ruling, and the cases were consolidated under the title **Mozilla v. FCC**.⁴⁴ In October 2019, the Federal Circuit Court of Appeals ruled that the FCC could reclassify ISPs as Title I or II but could not block state-level legislation enforcing net neutrality. Various states have enacted versions of net neutrality laws, but most work within the framework set by the FCC. For instance, California introduced **Bill SB822**, which restored on national level the rules of the 2015 Open Internet Order, passed with bi-partisan support, it became law in September 2018. Interestingly, on the very same day, the state of California was sued by the US Department of Justice as the latter argued that only the FCC had the authority to regulate broadband Internet

⁴² National Cable & Telecommunications Association vs. Brand X Internet Services, 545 U.S. 967, 2005.

⁴³ Verizon Communications Inc. v. Federal Communications Commission, 535 U.S. 467, 2002.

⁴⁴ Mozilla Corp. vs. Federal Communications Commission, 940 F.3d 1 (D.C. Cir.), 18-1051, 2019.

providers. Where more recent developments are concerned, in October 2020, the FCC voted in favour of reaffirming net neutrality regulations and, in February 2021, the U.S. DOJ dropped its lawsuit against California for its bill on net neutrality. Moreover, on 9 July 2021, the newly elected President J. R. Biden signed **Executive Order 14036, "Promoting Competition in the American Economy"**. The Order included instructions for the FCC to restore the net neutrality rules that had been reversed during the previous administration.

5.2.3 Digital platform regulation in the US system

a. Digital Platforms and Civil Liability

The starting point when analysing the US liability regime for digital platforms is **Section 230 of Title 47 of the US Code, enacted as part of the US Communications Decency Act⁴⁵**. Section 230 core rules can be found in Section 230(c) (1) and Section 230(c) known as the "Good Samaritan" clause. The first is of crucial importance in the debate as it provides immunity for website platforms with respect to third-party content, while the second, provides protection for operators of interactive computer services when removing or moderating third-party material they deem "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected", if they are acting in good faith. Nowadays, Section 230 has become particularly important in the debate around social media networks and their role in society. Those who criticise this rule argue that it grants too broad a protection to platforms, hence, allowing large tech companies to overlook the harm that users may suffer.

It should be noted that the immunity granted by Section 230 is not unlimited and specific exceptions regard federal criminal liability, electronic privacy violations and intellectual property claims. In addition, service providers must comply with some additional copyright requirements since the enforcement of the Digital Millennium Copyright Act in 1998⁴⁶. While the discussed section managed to grant service providers almost complete immunity in its first decade of existence, starting from the late 2000s new case law established that providers could be held liable if they are "publisher or speaker" with regards to the content published by the users⁴⁷.

Following, new limits were introduced to Section 230 as a response to the rising concern of Americans on content related to sex trafficking and child abuse. Advocates against sex trafficking and sex exploitation tried pressuring major websites to remove and block such content, and even though some major players introduced a stricter scrutiny, the debate around website liability and Section 230 did not cease. Section 230 was amended in 2018 by two bills, commonly referred to as the **FOSTA-SESTA package**, which include the **Stop Enabling Sex Traffickers Act (SESTA)** and the **Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA)**. The two combined bills

⁴⁵ 47 U.S. Code § 230 – *Protection for private blocking and screening of offensive material*

⁴⁶ Public Law, 105–304, Oct. 28, 1998 – *Digital Millennium Copyright Act*

⁴⁷ See: *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* 521 F.3d 1157 (9th Cir.) 2008.

require the removal of online material violating sex trafficking laws and amended the scope of Section 230 in that service providers who consciously help or support sex trafficking or other related illegal content are no longer protected by Section 230 immunity.

More recently, in February 2020, the US DOJ organised a workshop on Section 230 and, in June, presented some recommendations on how to modify the discussed section. These included how to give incentives to platforms to detect and remove illicit content, how to remove protection when civil lawsuits are brought by the federal government, or remove Section 230 protection in antitrust actions against large platforms, and better define existing terms and require platforms to publish how they moderate content. In May 2020, President Trump issued an executive order targeting Section 230 and the social media,⁴⁸ then rescinded by the newly-elected POTUS. Today, reforming Section 230 is on the agenda for both the Congress and the Biden administration. Recent proposals to reform Sections 230 can be divided into four main categories: (i) bills to repeal Section 230; (ii) bills to restrict the scope and the actions protected by Section 230; (iii) bills to impose new duties on companies that want to use Section 230 in their defence; (iv) bills to alter the “Good Samaritan” clause. Some of the many proposals currently aiming to reform Section 230 are: (a) the **Earn It Act**, with bipartisan sponsorship, this Bill would exclude Section 230 protection in case of violations of child sexual abuse laws; (b) the **SAFE Tech Act (Safeguarding Against Fraud, Exploitation, Threats, Extremism and Consumer Harms Act)** which would reform Section 230 and allow digital platforms and social media to be held liable for enabling cyber-stalking or discrimination on their platforms; (c) the **Accountability for Online Firearms Marketplaces Act**, which aims at removing Section 230 for firearm marketplaces operating online.

b. Digital Platforms and Freedom of Speech

In the public debate on regulating website platforms, a fundamental keystone is provided by the **First Amendment of the US Constitution**, which prohibits the government from restricting most forms of speech, including proposals that would force tech companies to moderate content. The First Amendment is often recalled in connection with Section 230, even though the issue of freedom of speech is at least partially distinct from the issue of whether digital platforms should be liable for what their users post. The First Amendment prevents the U.S. Congress from passing laws that restrict freedom of speech and this protection is extended to states and local governments thanks to the **State Action Doctrine** and the **Due Process Clause of the Fourteenth Amendment**.

The State Action Doctrine does not extend the application of the First Amendment to private parties, such as individuals or private companies, as only the government can violate an individual’s freedom of speech. In this, it should be noted that the social media is officially neither a public nor state actor, and its platforms are not considered public forums under current regulations, which means what users post on such websites falls outside the scope of the First Amendment and its protection of free speech. There are, however, three exceptions to the State Action Doctrine: (a) the exclusive

⁴⁸ EO 13925 – *Executive Order on Preventing Online Censorship*, May 28, 2020.

Public Function Doctrine, which refers to when a private party exercises a function that is traditionally reserved to the state to limit freedom of speech; (b) the entanglement exception and (c) entwinement exception which occur when the state is strongly involved, or entangled itself, with the private actor that has restricted freedom of speech. Moreover, when speech takes place in a public forum, it can qualify for protection of speech under the First Amendment⁴⁹. According to the Public Forum Doctrine, a speech can qualify for protection of speech under the First Amendment if it takes place in a public forum. While private facilities are not protected by this principle, social media platforms have often been characterised as a “digital public square”, yet this view has been rejected so far by the U.S. courts.⁴⁹ Traditionally, it is possible to identify some categories of content-based restrictions of speech that have been allowed, namely: (a) defamation, misinformation, perjury, fraud, government officials; (b) hate speech and speech that incites imminent lawless action; (c) advertisements (which are only partially covered by the protection of the First Amendment).

With regards to social media and freedom of speech, some important state-level legislation should also be recalled. Firstly, **Florida’s Bill SB 7072 on Social Media Platforms** was recently approved, requiring social media platforms to meet certain requirements when restricting speech by users, and establishes restrictions on contracting with public entities for social media platforms which have previously violated antitrust laws. Under Bill SB 7072, the Attorney General of Florida will have the power to bring action against companies that violate this law, and if social media companies are found to have infringed antitrust law, they will not be allowed to contract with public entities. Moreover, citizens of Florida who suffered unfair treatment from large tech platforms will be able to sue companies that violate their rights and receive monetary compensation if they win the case. Finally, the bill prohibits such companies to de-platform political candidates of Florida and, in case of violations, the Florida Election Commission will have the power to impose fines ranging from \$25,000 per day (in the case of candidates running for non-state-wide offices) up to \$250,000 per day (in the case of candidates running for state-wide offices).

Another important example is **Texas’ Bill HB 20 “on censorship of or certain other interference with digital expression, including expression on social media platforms or through electronic mail messages”** that was made law on 9 September 2021 by the Texas Governor. Under Bill HB 20, social media companies are forbidden to censor or restrict user content based on “the viewpoint of the user or another person.” Moreover, the bill requires extensive public disclosure of moderation practices of large social media platforms (i.e., platforms with more than 50 million monthly users in the U.S.), create a complaint system and display their content regulation procedures. Texas residents who have been “wrongfully” censored due to political ideas can either sue social media actors directly or allow the attorney general to bring action on their behalf. The most obvious challenge to both these bills is the conflict with Section 230 and, currently, both state laws have been contested in court, with the resulting litigation being likely to make it through to the Supreme Court.

⁴⁹ Recently, an appellate court held that the official Twitter account of the back then President of the United States was a designated public forum. See: *Knight First Amendment Institute v. Trump*, 928 F.3d 226, 2d 2019 (petition for cert. pending.)

c. Digital Platforms and Market Power

Digital markets have become a crucial part of our economy, with large tech companies and mergers involving digital platforms drawing increasing attention from US antitrust agencies in the last years. Proof of this heightened interest can be found in the series of hearings, held by the Federal Trade Commission (FTC) in October 2018, on multi-sided platforms and nascent competition in platform markets. Later, in February 2019, the FTC announced the launch of a new task force to monitor tech-markets, including online platform markets. The new task force focuses exclusively on these markets, verifies if tech companies abide by antitrust laws by reviewing prospective and consummated tech-mergers, and has the authority to act if breaches are detected. Later in the same year, the FTC and the Department of Justice (DOJ) decided to split their jurisdiction over the firms that control online platforms in order to better evaluate their anti-competitive conduct under the Sherman Act or the Clayton Act. The FTC oversees Amazon and Meta, while the DOJ focuses on Google and Apple⁵⁰.

Following, in October 2020, the House Committee on the Judiciary's Subcommittee on Antitrust, Commercial and Administrative Law presented a report (preceded by a 16-month investigation) on anti-competitive practices in the digital field, and several proposals of measures to address the issues which presented an in-depth analysis on the current challenges and key issues regarding antitrust rules and the market power of large Internet companies.

During 2021, several bills directed at large platforms and intermediaries were presented, both from the House of Representatives and the Senate. Some of these bills seem to rely on bipartisan support and resemble provisions included in the DSA and DMA on the other side of the Atlantic. Included in the different proposals, there is: (a) the **American Innovation and Choice Online Act**, which will limit companies from giving preference to their own products or services, and forbid companies from using data they collected from companies on their platforms in order to develop competitive products; (b) the **Platform Competition and Opportunity Act**, which shifts onto large digital platforms the responsibility to prove the legality of a merger; (c) the **Ending Platform Monopolies Act**, which targets Big Tech's presence across multiple industries and would stop these companies from favouring their own services; (d) the **Augmenting Compatibility and Competition by Enabling Service Switching Act (ACCESS Act)**, which would force companies to create new interfaces that allow their users to transfer personal information between different platforms; (e) the **Merger Filing Fee Modernization Act**, that would change the fee structure for pre-merger notification filings and increase the annual budget for Antitrust Divisions of the FTC and the DOJ.

⁵⁰ See, for instance: "CNN – Google, Facebook and Apple could face US antitrust probes as regulators divide up tech territory" available at: <https://edition.cnn.com/2019/06/03/tech/facebook-google-amazon-antitrust-ftc/index.html>

6. Resetting EU-US relations: common ground and challenges

6.1 The EU's perspective on digital spaces and markets

6.1.1 European digital transition: investments and projects to close the gap between the EU and its competitors

Apart from all its competitive disadvantages, it is clear that the EU is proposing initiatives that may strengthen its digital sovereignty and help put it back at the forefront of technological development.

Horizon 2020 is an €80 billion fund to invest over a period of seven years in research and development projects to secure Europe's global competitiveness. The European Investment Council was established under the Horizon programme and has a €10 billion budget to fund the development of new advanced technologies.

Another important project is the **Gaia X project**, jointly launched by Germany and France, that intends to create a sovereign cloud and digital ecosystem which will allow data to be shared in a trustworthy environment. Apart from the Gaia X initiative, the EU has also launched the "European Alliance on Industrial Data, Edge and Cloud" which supports industries, experts, MSs and other relevant stakeholders in developing cloud and related technology in a cooperative setting.

In the field of semiconductors, the EU has recently launched the "**Industrial Alliance for Processors and Semiconductor Technologies**", whose purpose is to identify and solve gaps in the design and production of microchips. The Alliance will work on the reinforcement of design and manufacturing of the most advanced types of semiconductors.

Where 5G is concerned, the European Commission has launched the 5G PPP initiative. Together with the private sector, its objective is to develop solutions in the telecoms field and to ensure that Europe is at the forefront of new markets such as smart cities. The 5G PPP counts with €1.4 billion to develop innovative communications infrastructure and 5G standards.

The EU has also put forward several initiatives for investing in new technologies such as AI and blockchain. Horizon 2020 allocated €1.5 billion to AI between 2018 and 2020, and the EU's Multiannual Financial Framework will add € 2.5 billion to invest in the use of AI by public administrations.

With these initiatives, the EU should build on its competitive advantages, namely the demand-side economies of scale potentially provided by one of the largest internal markets on the globe. However, more is needed to overcome its fragmentation across national boundaries, including cultural and linguistic barriers.

In the past, the EU supported many “upstream” investment projects, however, radical change is required in order for the EU to catch up “downstream”. In order to keep up, it must invest in building a strong digital ecosystem, including the demand side. Europe has comparative advantages in the field of operational technologies, such as 3D printers or smart robots, as well as a strong research community. However, a large share of businesses and citizens still lack the knowledge, or even the possibility, to take part.

Overall, **there are positive signs that Europe is becoming a more attractive economy to invest in, as investment in EU start-ups is growing -they hit a record \$34 billion in venture capital in 2020.** The EU does not need to create its own European Google to become a technological superpower, but, instead, should make sure that the competitive conditions are such that one could emerge.

By leveraging its competitive advantages, namely by investing more in its operational technologies, where it is more likely to become a world leader (although China is investing widely in operational technologies, the US is behind Europe in this field), **the EU may actually come to dominate an important area of technological development.** At the same time, the Union has the tools to create a trustworthy digital environment for investors, companies and consumers, which will certainly attract more capital and players to its internal market.

6.1.2 The EU’s view on a fair and safe digital landscape

The EU envisages a digital space that is safe for users and respects the EU values of democracy and human rights. In order to achieve this, it has to address several challenges and threats that arise from the digital economy - the EU digital markets, the level playing field for competition, the protection of EU values and human rights.

To this end, the Union has taken a regulatory approach to defend security and fundamental rights, and to ensure the stability of its democracies and economies.

In order to achieve the above, the EU has developed a comprehensive framework of regulations, which cover challenges raised by the surge of the digital economy and platforms. The first landmark regulation to enter into force was **“The General Data Protection Regulation” or GDPR.** The GDPR was launched **in 2018**, and it became the first comprehensive piece of regulation addressing the privacy and security of EU citizens.

In the same year, the EU adopted the Networks and Information Security Directive or NIS, which intends to boost cybersecurity across the EU. **A new legislative proposal (NIS II) covering cybersecurity and critical infrastructure protection has been presented to replace the NIS Directive with an improved and updated framework.** In the field of cybersecurity, the EU has also

put forward, the **Cybersecurity Act (adopted 2019)** which creates a cybersecurity certification framework from products and services circulating in the EU.

More recently, and taking into account the increasing importance of Digital Markets and Services in the lives of citizens, companies and states, the EU has launched a comprehensive set of initiatives to regulate its digital markets and services. The initiatives are also known as the Digital Services Act package and include two directives - the **“Digital Services Act” or DSA** and the **“Digital Market Act” or DMA**.

In the context of the European strategy for data, the Commission has introduced the Data Governance Act to regulate the share of industrial data within the EU. More recently the Commission announced it will be proposing an **AI legislation for high-risk applications**.

Apart from the above-mentioned initiatives, the EU has published a toolbox on 5G cybersecurity to guarantee that MSs do not opt for hardware provided by entities, which may be legally bound to share sensitive data with their governments. Although, not directly mentioning China, it seems it is the intention to warn MSs of the dangers in opting for providers such as Huawei.

The EU has also created a framework for filtering foreign investment, namely, if such investments are performed by state-owned or state connected entities, when those states are not democratic (such as China) or from dominant players for market domination purpose.

By approving such a robust regulatory framework, the EU intends to become a safe space for both companies and users, which attracts investors from all over the world while ensuring that European democratic values are respected.

6.2 The Trade and Technology Council (TTC)

6.2.1 Background and relevance

During the EU-US summit in June 2021, Presidents Von der Leyen and Joe Biden committed to renewing the Transatlantic Trade Partnership, and to set the agenda for future talks for the worlds' biggest trading partners.

The renewal announcements came after several setbacks that marked the Trump administration's approach on the transatlantic trade relations (e.g. sanctions on imports of steel and aluminium), and other long-standing trade discussions such as the Airbus/Boeing dispute.

One of the top priorities identified during the summit was to boost commercial and technological cooperation in strategic fields. The digital economy is central for both the US and the EU. The EU and the US are the largest trading partners in the world. In 2020 alone, the US exported a total amount of \$248 billion in ICT and potentially ICT-Enabled Services to Europe, while it has imported \$142 billion from Europe.

To formalise the “new era” of EU-US trade cooperation, the parties decided to establish the **Trade and Technological Council (TTC)**. The TTC was set up to foster common investment in forefront technologies, to reinforce supply chain resilience, and to ensure further cybersecurity resilience for both sides.

Both the EU and the US share common values of freedom and democracy and are like-minded partners in the protection of human rights in technological development. Based on these common values, the TTC intends to become a platform that ensures beneficial trade and technology policies for both parties. It is a promising platform to strengthen transatlantic commercial ties, based on liberal democratic values and respect for human rights.

The TTC will be made up of several working groups, each focusing on developing discussions around a specific priority.

6.2.2 Structure and priorities

Ten working groups will be responsible for developing the activity of the TTC. The working groups will focus on digital related topics ranging from cybersecurity to supply chain resilience especially regarding the production and supply of semiconductors.

It is not yet clear who exactly will be involved in the working groups, but it is now clear that the working group activity will entail consultation with stakeholders as well as political dialogue on each working area. Senior officials from both the US and the EU will lead the working groups. While the US has not yet released information on who will be coordinating the working groups on the American side, the EU has selected Commission senior officials from several Directorate-Generals, such as DG GROW, DG COMP, DG CONNECT, as well as from the EU External Action Service.

The TTC’s working groups will promote a strong involvement of stakeholders, and work together with those same stakeholders on developing outputs that are beneficial to all parties. During the Council’s meeting, the EU and US leaders defined the TTC’s priorities, concrete deliverables as well as the tasks of each working group. At the end of the encounter, the parties released a joint statement identifying five key areas of cooperation.

In the area of export controls, the US and the EU have agreed to enhance control over the trade on dual-use items (i.e. items that may be used for both civilian and military purposes). The action in this field focuses on introducing export controls on sensitive technologies such as cyber surveillance technology, and increasing cooperation to ensure best practices on both sides and that the partners’ common values are respected.

Although the joint statement does not refer to China directly, the concern regarding cybersecurity technology may be related to China's potential ability to collect US and EU citizens' data from the database cybersecurity companies, such as Hikvision. The US has recently banned American investment in the Chinese company, which supplies cameras to several EU MSs, based on the accusation that the company was collaborating with Chinese authorities on the mass surveillance of the Uyghur population.

Foreign direct investment (FDI) screening is another area of great concern for both sides. The EU's FDI screening regime entered into force in October 2020 to facilitate investment screening in the EU. The EU intends to ensure that the investments performed in its internal market do not jeopardise Europe's security or public order. On the other hand, the US has recently modernised its existing investment screening regulation (FIRRMA), and approved measures that apply to certain FDI involving US businesses that produce strategic technologies. Through the TTC, the US and the EU expect to agree on basic principles and best practices for investment screening.

Semiconductors are extremely important for both the US and EU economies. These micro-chips are a key component for the production of most electronic devices ranging from medical and military equipment to mobile phones. The EU is largely dependent on external players to obtain semiconductors. From a 44% market share in the 1990s, it has now dropped to below 10% of worldwide production. Taking into consideration the strategic importance of semiconductors, the EU has announced the release of a **European Chips Act** which is focused on increasing its production and reaching 20% of global manufacturing by 2030. The European Chips Act intends to increase semiconductor production capabilities, research and supply chain resilience.

The US used to produce 37% of the total chip production, but now only produces 12%. While China is currently responsible for the production of the same percentage, it is investing heavily in chip production, and its share could increase to 28% of the global production by 2030. Similar to the EU, the US has also launched its own CHIPS for America Act, which has recently received \$52 billion in financing. The US CHIPS Act will address the areas of research and supply chain resilience.

Securing semiconductors is fundamental for the US and EU's strategic autonomy connected to the European chip policy. **Through the TTC, both parties intend to increase cooperation on enhancing design and manufacturing domestic capacity to rebalance global semiconductor supply chains.**

Another area where the interests of the US and the EU are aligned is the definition of **global standards for Artificial Intelligence and other emerging technologies**. Both parties agree that AI is a powerful technology that can result in significant improvements in the lives of EU and US citizens. Nevertheless, it is also clear that AI may also threaten liberal democratic values and human rights. Proof of such a "dark side" was the use of AI systems as a form of influence vote on the Brexit referendum and on President Donald Trump's campaign in 2016, as well as the January 6 invasion of the US Congress.

The EU has recently launched a legal framework on AI that intends to ensure that this technology may be used without harming the EU's values. The framework will use a risk grading system to determine the requirements of AI providers before they commercialise their products in the EU internal market. The US has also presented initiatives such as the AI Risk Management and the US National Initiative on AI, which intend to guarantee that AI technologies are trustworthy and follow strict standards of transparency and fairness.

On the TTC joint statement, the EU and the US have affirmed their willingness to cooperate on critical standards in emerging technology, especially in AI. The cooperation on AI will be based on a human-centred approach that enhances shared democratic values and protects citizens' human rights. Among other initiatives, the EU and the US have committed to discussing evaluation tools to assess requirements for trustworthy AI, that is, to tackle bias mitigation.

6.2.3 Challenges

Despite their common objectives, the EU and the US disagree on certain points, such as regulation of "big tech" companies or their approach towards China. To reach fruitful outcomes, the two must find constructive solutions to address these issues.

Where **China** is concerned, the US generally has more of a competitive no dialogue approach. Instead, the EU is open to dialogue to ensure that economic relations are maintained while political and diplomatic issues are treated in parallel. However, no common approach exists between EU Member States.

The TTC's joint statement does not directly mention China, however, it is clear from the priorities established that there is concern regarding Chinese companies operating in the EU and the US due to their close connections with the Chinese government.

Apart from different approaches to China, other geopolitical episodes may also interfere in the TTC's activity. An example of such a situation was France's request to postpone the first meeting of the TTC due to the agreement between Australia, the US and the UK (the so-called AUKUS) which led to the cancellation of a submarine deal between France and Australia.

However, it is on regulatory matters that the US and the EU most diverge. The EU's regulatory approach to digital markets and platforms is often viewed as protectionist towards American businesses.

The Digital Service Act Package was proposed by the European Commission on December 2020 and includes two legislative initiatives that aim to create a regulatory framework for digital companies

acting within the EU. The package includes two initiatives - **The Digital Services Act (DSA)** and the **Digital Markets Act (DMA)**.

The DMA will regulate digital markets, and has the objective of establishing a level playing field to foster competitiveness and innovation within the EU internal market. The EU intends to build a fair and competitive digital ecosystem, by directly targeting the economic dominance of Large Online Platforms (LOP), which according to the European Commission have “emerged as gatekeepers in digital markets, with the power to act as private rule makers”. The LOP business model is based on the extraction of user data, which is then used in “behaviour futures”. LOPs then sell these insights to other companies, which look for accurate targeted advertising.

The so-called “data power” creates distortions in competition in favour of LOPs as these control most of the existing data flows and, therefore, most of the profits generated with data. The EU considers that the fact that only a few LOPs control large parts of the digital economy, results in a clear disadvantage for smaller businesses, and less alternatives for consumers.

The issue here is that most LOPs operating in the EU internal market are US companies. The so-called GAFAM (Google, Apple, Facebook, Amazon, Microsoft), dominate most of the digital market in the EU and would be most affected by the DMA. Although the regulation of digital markets is convenient to both parties, as it spurs competitiveness and innovation, the DMA proposal is seen as protectionist towards US big tech companies.

The same principle applies regarding the DSA. The DSA proposes the creation of a set of rules to avoid disinformation and improve transparency on the algorithms used by social media, search and e-commerce. The DSA will replace the E-commerce Directive, which the Commission believes is outdated and unable to cope with the new challenge of the digital ecosystems.

The new directive will establish reporting and transparency requirements for LOPs in order to guarantee that respect for fundamental rights and EU values are safeguarded for European users. Among the proposals put forward by the directive is the establishment of due diligence procedures to tackle illegal content, or the publication of the algorithms used for the content moderation upon request from the Commission.

The DSA creates specific obligations and higher standards for certain “very large online platforms” (with over 45 million users or 10% of the EU’s population). According to the Commission, due to their size, these platforms are subject to higher risks of manipulation from third parties. Therefore, the DSA creates mechanisms for those platforms to be able to assess risk of interference and further requirements for user protection.

The US does not have any similar proposals on the table and believes that the EU’s regulatory approach is a barrier to innovation and to the development of new competitive players in the field.

The DSA is viewed as creating unnecessary and disproportional burdens on digital companies operating in Europe. Moreover, the US views the thresholds for defining very large companies as directly targeting US big tech players, putting them at a disadvantage when compared to other platforms.

Finally, there is the issue of **data flows between the US and the EU**. The EU used to rely on two legal frameworks to ensure the respect for EU citizens' privacy rights. However, both the Safe Harbour (2000), and its replacement the Privacy Shield (2016) were invalidated by the European Court of Justice (ECJ), respectively, in the Schrems I (2015) and in the recent Schrems II cases (2020). In Schrems II the court considered that the US legal framework does not offer EU citizens the same protection that is provided by EU law and more specifically by the GDPR.

The ECJ based its decision on the US legislation that gave the US authorities access to data imported from the EU (Section 702 FISA). According to the court US, legislation did not have the adequate controls to protect EU citizens' data to be targeted for investigation in national security related issues.

Due to the importance of data transfers between the EU and the US, in Schrems II the ECJ has allowed transfers to go on under GDPR art. 46 transfer mechanisms, as long as the transferor is able to put in place the adequate safeguards to make data transfers impossible. However, this is a temporary measure and it is urgent that the US and the EU agree on a new framework for data transfer, otherwise businesses may be affected.

6.2.4 Expected developments in the near future

The TTC may indeed be a positive step towards restoring sound commercial relations between the EU and the US. The Joint Statement, issued after the first meeting of the TTC, has demonstrated that there are several areas in which the partners agree that work needs to be done and that common solutions should be found.

The Joint Statement has revealed the objectives as well as the strategy of the TTC. The partners intend to work closely with stakeholders, industry and civil society and reach concrete solutions on the five key areas referred to above. The TTC is also focused on finding like-minded partners in other jurisdictions that are willing to cooperate in the creation of technological standards based on liberal democratic values.

In order for the TTC to thrive, and for the common objectives to be reached, the US and EU should work together in finding common ground on the regulation of data-based businesses and digital markets. This should be done in the knowledge that there are different interests and different approaches between the EU and US when dealing with digital markets, namely digital sovereignty

or digital autonomy. These differences should be clearly acknowledged, because they were in the past, and may be in the future, the source of tensions. However, there are clearly domains in which a compromise between EU and US objectives can be reached.

The US and the EU have different perspectives on regulation of digital platforms and the digital economy in general. While the EU believes that the digital realm raises new challenges for competition policy that should be addressed by proper and updated ex-ante regulation, the US often regards the digital sector as just another sector of the economy and that new regulation will only create unnecessary burdens and restrain innovation and growth.

Reaching an agreement on a common regulatory framework for the digital world will therefore be hard, as the EU and US approaches seem difficult to align. Even though the TTC has a specific group to deal with “Data Governance and Technology Platforms”, the TTC’s Joint Statement specifically refers to the parties’ regulatory autonomy in several places.

The EU could also push for an acknowledgement by the US that its policies are not meant to be protectionist and directed only at US businesses. In fact, the overarching aim of the Digital Services Act Package is to control the activities of all companies (both EU and US) providing digital services to EU citizens and businesses.

Although a Joint Technology Competition Policy Dialogue was established in parallel with the TTC, the parties have already made it clear that it will not lead to common legislation.

Finally, the issue of a common framework for data governance is also not likely to be solved in the context of the TTC. The Joint Statement is vague on this topic - once again, the parties disagree on key aspects. In particular, the EU wants legal commitment from the US that EU citizens’ data will not be accessed by US agencies. However, legislation that allows for such protection is unlikely to pass in the US Congress. This is due to the fact that US officials consider strict rules about data governance as potentially undermining the action of intelligence and other agencies in ensuring national security, making it harder to reach consensus on this topic. For these reasons, it seems likely that the Privacy Shield stalemate will not be addressed in the context of the TTC.

Conclusions

This paper explores the concept of **digital sovereignty** applied to the European Union, placing the current policy initiatives, regulatory interventions and international relations, especially with the US, in this context. **It is the result of the collaboration of four think tanks from Southern Europe (Greece, Italy, Portugal and Spain), sharing some common problems and challenges.**

In the paper, we highlight the **need to distinguish between two ideas which pertain to different areas of analysis and policies.** First, the issue of European digital sovereignty, that is, how to foster European companies through regulation, industrial policy through a case study, and outwardly multilateral mechanisms. Second, on the other hand, the issue on how to digitalise European assets inwardly.

The starting point is that the EU has fallen behind its main competitors in almost every important aspect of the digital economy. Its dependence on third parties for obtaining strategic digital assets and technology is a threat to its ability to act autonomously. Moreover, the excessive dependence on third parties is also a threat to the EU's core values and the functioning of its democracies. To face the challenges arising from the digital transformation, Member States and EU institutions have presented several regulatory and investment initiatives aimed at strengthening the EU's competitiveness in the digital realm and guaranteeing that digital players respect EU values.

Europe, indeed, has an opportunity to recover its lost technological, especially digital, ground. The failed Lisbon Agenda of 2000 is being replaced by a Path for the Digital Decade with proposals of new methods of governance and new public and private resources which could help to realise the idea of European Digital Sovereignty or autonomy. However, the latter cannot be locked in on itself. It must be open to other countries and regions, in particular, the US. Hence, the idea of Open Strategic Sovereignty, in this field (and others).

The regulatory power of the EU should not only be geared to its digital, technological and industrial interests, but also to defending democratic and citizen values, human-centred tech, privacy, transparency and other principles, related to establishing the EU's international positioning in the technological realm by means of bilateral agreements and multilateral mechanisms.

DIGITAL COMPETITIVENESS

Digitalisation could act as an enabler for economic growth and development, though its implementation faces many challenges. The pandemic has exposed the need for digital technology even for the most traditional sectors. However, Europe's digital sovereignty is in question since it seems that in certain key areas, the EU and, overall, the southern states, remain (significantly) behind the global digital leaders.

On most digital economy indexes, the US scores the highest, while China is catching up, especially after the outbreak of the pandemic. Using the I-DESI index, the top four countries of the EU average rank in the three first positions, while Switzerland, Norway and Iceland also show a superior performance. On the other hand, the EU bottom MSs' average score falls towards in the tail-end of the ranking. **The great disparities among the EU countries, particularly between Northern and Southern MSs, are a great obstacle to promoting the EU as a digital leader and, as well, does not contribute to economic convergence within the EU.** In connectivity, the total EU27 average compares well with non-EU countries, while in human capital, 10 of the 18 non-EU countries had a higher score in 2018. In the use of Internet services, non-EU countries generally perform better than the EU27 states.

In particular, European companies are less mature than their counterparts in other advanced economies in their adoption of digital technologies and the use of those technologies for new services and business models.

A critical factor for success on the digital route is the development and adoption of AI technologies. The EU had traditionally been a leader in AI research, but since 2017, China has led the field of peer-reviewed AI publications, with the gap growing in the years since. Moreover, the US is leading worldwide in patent applications, while China is more prominent in data collection and data access, the main source for developing AI technologies. Therefore, Europe should focus on regaining a leading position in AI research and, at the same time, to provide a policy framework that encourages corporate-academic synergies and the commercialisation of research outputs.

To explore further the determinants of digital adoption by firms, we have used the data of the I-DESI for the period 2015-2018. The objective is to identify the key factors that enable firms to successfully adopt digital tools. We find that if a government aims to increase its adoption of digital technology, **the critical factors in climbing the ranking of the I-DESI, *ceteris paribus*, are the dimension of citizens' use of the Internet, in general, and when considering the sub-dimensions:** a) fixed broadband take-up; b) mobile broadband take-up; c) at least basic skills; d) at least basic software (coding); and e) fixed broadband traffic.

DATA INFRASTRUCTURES

Access to data and its use is a key area where to improve digital competitiveness and achieve an open digital sovereignty. There is no single solution or set of "formulas" to make European companies leaders in cloud computing, the main technological platform to access data and embrace digital transformation, **or to consolidate new publicly-led proposals in the long run with specific mandates, timings and allocated resources.** However, the analysis of previous attempts by MSs (e.g., Andròmede, De-Mail and Quaero) highlights what should not be done, or what should be newly created, in current attempts to advance the European quest to improve its positioning in the global tech race through GAIA-X, the IPCEI-CIS and the European Alliance on Data, Edge and Cloud.

Several policy lessons underline the need to distribute competences in both leadership and implementation amongst larger companies and SMEs. The procurement role is more flexible as it depends on interactions between both the public and private sectors. Also, MSs should speed up in establishing a common Multi-Provider Cloud-Edge Continuum in order to offer a framework that is competitive in the presence of a growing and diversified cloud services portfolio which is offered by non-EU firms within Europe. As well, governments should start carrying out joint risk mapping, evaluate joint asset availability of technological capabilities by European firms, and develop an impact assessment following up on the interests and priorities of the EEAS, DG CONNECT, DG TRADE, as well as the Member States.

REGULATORY REFORM: AI Act, DSA, DMA

Alongside a data strategy, based on a mix of infrastructures and services, over the last year, the EU has launched several ambitious initiatives, such as **the DMA, the DSA and the AI Act**.

Generally speaking, **these proposals are highly appropriate and timely, stemming the current risks (and the increasing reality) of regulatory fragmentation**. However, the new regulatory framework, while needed to face the many risks entailed by rapid market developments, must also deal with the concrete possibility of unintended consequences that could stifle innovation and, paradoxically, competition.

Digital markets display high rates of dynamism and innovation, with an increasing speed of introduction and spreading of new services. **The relationship between innovation and competition is extremely complex, even more so in digital markets where new technologies risk becoming obsolete and outdated within a few years**. As for the market segmentation identified by the DMA, it is worth noting that it is extremely complex to identify clear boundaries and distinctions, for instance, between video-sharing services like YouTube and social networks like TikTok. Indeed, there are now numerous cross-sector platforms, which are continuously seeking to expand their range of services and aim at increasing user-friendliness, as well as customising their services to meet new trends or consumer preferences.

Thus, **regulation should not reduce the spectrum of choices available to consumers by stifling innovation and, in doing so, achieve the opposite** (i.e., as could happen if targeted advertising or recommender systems are banned or severely restricted).

Measures such as those contained in art. 5 and 6 of the DMA should take into account the need to protect the integrity, security, and quality of digital services supplied by the gatekeepers, as well as the rights of business users and end users.

At the same time, **for instance in areas such as AI, regulation is a necessary, but yet not sufficient framework to address the whole issue**. A broader scope is needed by combining regulation - which may help the EU to introduce its own values on AI into the world- with new policy lines of work on the industrial side. If Europe wants to have a significant say in the field, this will never come about

unless it achieves a leading role in the development of AI technologies. What European and MS institutions need to take into consideration is that if the race in AI development accelerates, and the gap between the EU and other countries becomes even wider, this will most certainly also affect the chances for the EU to establish itself as a leading force in the AI regulatory framework. Therefore, **considerable and well targeted investments need to accompany any regulation.**

EUROPE'S GLOBAL ROLE AND THE FUTURE OF EU-US RELATIONS

Both investments and regulation occur not in a vacuum but in an inter-connected world, raising the need for an external strategy to deal with other initiatives put forward by other countries. If the EU reaches its objectives of becoming a pioneer in a well-thought-out regulatory framework for digital markets and services, as well as boosting its technological leadership, it may become an example for other nations worldwide.

The concept of an open European digital sovereignty is *tous azimuts*, not only towards the US - a close ally with which the EU shares many fundamental values -, but also other countries, including non-European companies.

Due to the global nature of the digital challenges, the EU needs to seek cooperation with like-minded partners to ensure that digital standard-setting is based on the values of liberal democracy. The Trade and Technology Council is a first step towards a closer collaboration between the EU and the US in setting the rules for digital spaces and markets. However, the two powers have so far revealed divergent views on digital regulation, based on cultural, social and economic differences, that have to be dealt with. To ensure that liberal democratic values prevail in the digital realm, the US and the EU must strengthen their alliance and seek compromise in finding effective formulas to regulate the digital space.

Bibliography

BMWi.de (2021). *IPCEI on Next Generation Cloud Infrastructure and Services* (May 25, 2021). Link: <https://www.bmwi.de/Redaktion/EN/Artikel/Industry/ipcei-cis.html>

Boukal, N. (2019). *What happened to the German project DE-Mail?* (September 10, 2019). Cryptshare.

Bremmer, I. (2021). *The Technopolar Moment: How Digital Powers Will Reshape the Global Order*, Foreign Affairs (November/December 2021).

Bughin, J. et al. (2019) Tackling Europe's gap in digital and AI. McKinsey Global Institute. Available online at: <https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-europes-gap-in-digital-and-ai>

Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, and Raymond Perrault, "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March 2021.

Del Castillo, C. (2021). *Más de 300 empresas en España se ofrecen para crear GAIA-X, la nube al margen de Amazon o Microsoft*, Eldiario.es (September 8, 2021). Link: https://www.eldiario.es/tecnologia/300-empresas-espanolas-ofrecen-crear-gaia-x-nube-margen-amazon-microsoft_1_8282483.html

DW (2006). *Europe's Quaero Project Aims to Challenge Google*, DW (March 9, 2006). Link: <https://www.dw.com/en/europes-quaero-project-aims-to-challenge-google/a-1928217>

EEAS (2020). *For a united, resilient and sovereign Europe (with Thierry Breton)*. HR/VP Josep Borrell (June 9, 2020). Link: https://eeas.europa.eu/headquarters/headquarters-homepage/80567/united-resilient-and-sovereign-europe_en

European Commission (2020). *The International Digital Economy and Society Index (I-DESI)*. <https://digital-strategy.ec.europa.eu/en/library/i-desi-2020-how-digital-europe-compared-other-major-world-economies>

European Commission (2020). *State of the Union's Speech by President Ursula Von der Leyen* (September 16, 2020).

European Commission (2021). *State of the Union's Speech by President Ursula Von der Leyen* (September 15, 2021).

Goujard, C. & Cerulus, L. (2021). *Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project*, POLITICO.EU (October 26, 2021). Link: <https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/>

INPLP (2020). *GAIA-X: European sovereign cloud guidelines unveiled* (August 17, 2020). Link: <https://inplp.com/latest-news/article/gaia-x-european-sovereign-cloud-guidelines-unveiled/>
Johansson, B., C. Karlsson, M. Backman and P. Juusola (2007). *"The Lisbon Agenda from 2000 to 2010"*.

CESIS. Electronic Working Paper Series. Paper No.106. <http://www.diva-portal.org/smash/get/diva2:487429/FULLTEXT01.pdf>

Jorge-Ricart, R. (2020). *GAIA-X: an opportunity for the European digital sovereignty?*, Elcano Royal Institute (June 16, 2020). Link: <https://blog.realinstitutoelcano.org/en/gaia-x-an-opportunity-for-the-european-digital-sovereignty/>

Juncker, J-C (2018). *State of the Union 2018. The Hour of European Sovereignty* (September 12, 2018).

Linklaters (2019). *US Cloud Act and GDPR – Is the cloud still safe?* (September 13, 2019). Link: <https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe>

Mazzucato, M. *The Entrepreneurial State* (2013), Anthem Press.

MINECO (2021). *El Gobierno de España impulsa un hub nacional de GAIA-X para desplegar la economía del dato y apostar por el liderazgo de espacios de datos en sectores estratégicos como turismo y salud*, Ministry of Economic Affairs and Digital Transformation, Government of Spain. Link: https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210623_np_hub.aspx

Sahin, K., & Barker, T. *Europe's Capacity to Act in the Global Tech Race: Charting a Path for Europe in Times of Major Technological Disruption*, German Council on Foreign Relations (April 2021).

Shannon, V. (2008). *Quaero gets off the ground to challenge Google*, New York Times (March 21, 2008). Link: <https://www.nytimes.com/2008/03/21/technology/21iht-quaero24.html>

Tricot, R. (2021), "*Venture capital investments in artificial intelligence: Analysing trends in VC in AI companies from 2012 through 2020*", OECD Digital Economy Papers, No. 319, OECD Publishing, Paris, <https://doi.org/10.1787/f97beae7-en>.

Vie Publique (2010). *Déclaration sur le déploiement de la fibre optique dans les zones moyennement denses...*, Vélizy (January 18, 2010). Link: <https://www.vie-publique.fr/discours/177909-declaration-de-mfrancois-fillon-premier-ministre-sur-le-dploiement>
Walt, S. *Big Tech Won't Remake the Global Order*, *Foreign Policy* (November 8, 2021).

Waters, R. (2021). *Google bets on the cloud breaking up*, *Financial Times* (October 14, 2021). Link: <https://www.ft.com/content/ab36b9e2-00e0-469c-9388-fa034f9bfd63>

WIPO (2019). *WIPO Technology Trends 2019: Artificial Intelligence*. World Intellectual Property Organization.

ZDNet (2012). *Cloud Andromède: un projet « sans avenir » qui déshabille les acteurs en place*, *ZDNet* (July 10, 2012).

Zhongming, Z., Linong, L., Wangqiang, Z., & Wei, L. (2020). *OECD Business and Finance Outlook 2020*.

Appendix

Data and Methodology

We employ International Digital Economy and Society Index (I-DESI) data which combines 24 indicators and uses a weighting system to rank each country based on its digital performance to benchmark the development of the digital economy and society. I-DESI measures the digital economy performance of the EU27 Member States and the EU, as a whole, in comparison with 18 other countries worldwide (Australia, Brazil, Canada, Chile, China, Iceland, Israel, Japan, Mexico, New Zealand, Norway, Russia, Serbia, South Korea, Switzerland, Turkey, the UK and the US). The I-DESI uses 24 indicators and a weighting system to rank each country based on its digital performance to benchmark the progress of the digital economy and society (see Tab 1).

I-DESI index	
Dimensions	Sub-Dimensions
Connectivity Dimension	1a1 Fixed Broadband Coverage
	1a2 Fixed Broadband Take-Up
	1b1 4G Coverage
	1b2 Mobile Broadband Take-Up
	1c1 Fixed (wired)-broadband speed; in Mbit/s
	1d1 Broadband Price Index
Digital Skills Dimension	2a1 At least basic skills (Word processing)
	2a2 Above basic (advanced spreadsheet skills)
	2a3 At least basic software (coding)
	2b1 Telecommunication emps FTEs
	2b2 ICT Graduates
Citizen Use of Internet Dimension	3a1 Internet Users
	3a2 Fixed broadband traffic (GB/mth/person)
	3b1 Video Calls
	3b2 Social Networks
	3c1 Banking
	3c2 Shopping
Integration of Digital Technology Dimension	4a1 Availability latest technologies
	4a2 Firm-level technology absorption
	4b1 SMEs Selling Online

	4b2 Secure Internet Servers per million people
Digital Public Services Dimension	5a1 eGovernment Users
	5a2 Online Service Completion
	5a3 Open Data OKF OECD

Tab 1: Dimensions and indicators examined by I-DESI, European Commission

The variables included in the analysis are all normalised (in the interval 0 to 1). Thus, the coefficients are comparable, and we can easily distinguish the gravity of each dependent variable. For modelling, we employ the between estimator, which is preferred to compare the average differences between individuals and, in our case, countries. It takes advantage of the cross-sectional dimension (differences between units) of the data by regressing the individual averages of y on the individual averages of x and a constant using OLS. The general expression of our models is:

$$\bar{y}_i = \beta_0 + \beta_1 \bar{x}_{1i} + \dots + \beta_k \bar{x}_{ki} + \bar{u}_i, \quad i = 1 \dots N$$

Where \bar{y}_i is the average of the dependent variable, $\bar{x}_{1i} \dots \bar{x}_{ki}$ are the average explanatory variables for i subjects and N observations. In our case, the dependent variable is the integration of technology by businesses, and as independents, we utilise the indicators of the I-DESI sub-dimensions. The integration of the digital technology dimension considers both the digitalisation of businesses and the development of e-commerce.

Results of the empirical analysis

Countries of I-DESI	The average performance of Integration of Digital Technology Dimension for the 2015-2018 period
<i>Poland</i>	0.1575
<i>Brazil</i>	0.1925
<i>China</i>	0.235
<i>Lithuania</i>	0.255
<i>Romania</i>	0.26
<i>Greece</i>	0.26
<i>Italy</i>	0.26
<i>Turkey</i>	0.27
<i>Serbia</i>	0.2875
<i>Russian Federation</i>	0.295
<i>Slovakia</i>	0.3025

<i>Bulgaria</i>	0.3075
<i>Mexico</i>	0.3125
<i>Cyprus</i>	0.3375
<i>Croatia</i>	0.34
<i>Malta</i>	0.345
<i>Slovenia</i>	0.3575
<i>Spain</i>	0.3625
<i>Czechia</i>	0.365
<i>Korea</i>	0.37
<i>Hungary</i>	0.395
<i>Portugal</i>	0.3975
<i>Chile</i>	0.405
<i>Latvia</i>	0.4125
<i>France</i>	0.4275
<i>Australia</i>	0.45
<i>Estonia</i>	0.455
<i>New Zealand</i>	0.4675
<i>Austria</i>	0.4725
<i>Ireland</i>	0.49
<i>Japan</i>	0.4975
<i>Belgium</i>	0.515
<i>Germany</i>	0.5325
<i>Canada</i>	0.5425
<i>Israel</i>	0.5625
<i>Norway</i>	0.585
<i>Denmark</i>	0.595
<i>United Kingdom</i>	0.6
<i>Luxembourg</i>	0.62
<i>United States</i>	0.6225
<i>Sweden</i>	0.6275
<i>Finland</i>	0.6475
<i>Switzerland</i>	0.68
<i>Iceland</i>	0.6825
<i>Netherlands</i>	0.7025

Tab 2: Country ranking according to the average performance of Integration of Digital Technology Dimension for the 2015-2018 period

	Integration of Digital Technology
Connectivity	0.355 (0.245)
Digital Skills	0.319 (0.190)
Citizen Use of Internet	0.688*** (0.140)
Digital Public	-0.074 (0.124)
Constant	-0.175* (0.096)
Observations	45
R-squared	0.769
Standard errors in parentheses	
*** p<0.01, ** p<0.05, * p<0.1	

Tab 3: Results of regressing integration of digital technology against the other for main dimensions of I-DESI

	(1)	(2)	(3)
	Integration of Digital Technology	Integration of Digital Technology	Integration of Digital Technology
<i>1a1 Fixed Broadband Coverage</i>	0.515 (0.313)		
<i>1a2 Fixed Broadband Take-Up</i>	0.463** (0.198)		
<i>1b1 4G Coverage</i>	-0.155 (0.199)		
<i>1b2 Mobile Broadband Take-Up</i>	0.319** (0.128)		
<i>1c1 Fixed (wired)-broadband speed; in Mbit/s</i>	0.246* (0.145)		
<i>1d1 Broadband Price Index</i>	-0.069 (0.060)		
<i>2a1 At least basic skills (Word processing)</i>		0.661*** (0.138)	
<i>2a2 Above basic (advanced spreadsheet skills)</i>		0.249	

		(0.163)	
2a3 At least basic software (coding)		0.144*	
		(0.083)	
2b1 Telecommunication emps FTEs		-0.178	
		(0.134)	
2b2 ICT Graduates		0.087	
		(0.087)	
3a1 Internet Users			0.244
			(0.155)
3a2 Fixed broadband traffic (GB/mth/person)			0.229**
			(0.088)
3b2 Social Networks			0.201
			(0.129)
3c1 Banking			0.065
			(0.108)
3c2 Shopping			0.098
			(0.202)
Constant	-0.227	-0.057	0.027
	(0.254)	(0.050)	(0.042)
Observations	45	45	45
R-squared	0.627	0.819	0.791

Standard errors in parentheses
 *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

Tab 4: Results of regressing integration of digital technology against the sub-dimensions of each main dimension of I-DESI