Facing the US and China, the European Union meets intractable dilemma to settle its Digital sovereignty

Sarah Guillou *

SciencesPo OFCE

Work in progress

June 3, 2024

Digital sovereignty means that a country has the capacity to control, to regulate and to protect the flows of data and information which circulate on its territory. Why does digital sovereignty matter for the economy ?

There is a general consensus which admits that data, information, and digital technologies which transform the latter into value, are an increasing source of value and wealth creation. Let's define digital economy such as all business activity which mainly uses data and information as a source of value, or uses and improves digital technology to exploit data and information. Digital economy is undoubtedly a main source of growth, through value added and productivity, a main source of capital accumulation and a main source of revenue. It might also be a source of welfare improvement and at least of standard of living's increase. A very large literature has showed that intangible investment (Griliches 1998, Haskel & Westlake 2017, Ding et al. 2022), ICT investment and now Artifical Intelligence (Brynjolfsson et al. 2023, Noy & Zhang 2023), are to be drivers of productivity gains.

But the question whether digital sovereignty is necessary to benefit from the digital economy's productivity gains is not clearly established. We observe that industrial policies which intend to support the digitalization and boost the digital economy lie on the concept of digital sovereignty to justify the economic intervention.

Undoubtedly digital sovereignty should be a strong concern for sovereign governments for at least three reasons associated with the characteristics of the digital economy: (i) the tremendous economic power of digital private business caused by the platform growth model and the mastering of increasing level of technicity; (ii) the tendency of weaponization of the digital economy by a government against the sovereignty of another one; (iii) and the fact that digital economy is

*sarah.guillou@sciencespo.fr – OFCE, 10 place de Catalogne 75014 Paris.

dealing largely with sovereign missions such as create financial means, inform and archive public data (see Guillou 2023).[1]

But still, the economic benefit of digital sovereignty is to be assessed more clearly while the EU is facing strong contenders from the US and China.

This paper aims to explain why and how digital sovereignty mostly depends on economic issues and whether European policy decisions could enhance digital sovereignty. It **first** explains what is meant by digital sovereignty and whether the latter could be quantitatively measured. We argue that digital sovereignty is simultaneously a matter of law and regulation, a matter of technology skills but also of infrastructure and a matter of technological competitiveness (Corrado et al. 2016). We assess the strength of the EU relative to the US and China in these respects. **Then,** the paper highlights in which domain the state sovereignty is threatened by the digital economy focusing on tradition State's regalian missions. **Last,** it exposes how the EU policies should be designed to face the technical, the balance of power and the economic challenges brought by the international digital competition. We expose the intractable dilemma and the necessity to change the scale as well as to stick to European values to guide policies.

We finish with the necessity to stick to Europe principles to guide the design of policies: protect the integrity of information which is a pillar of European institutions, protect the competition and keep fighting against the abuse of dominant position and feed the scientific and enlightment legacy of the continent through a massive investment in education.

Section 1. What would be the attributes of digital sovereignty in general ?

1.1 What does digital sovereignty mean and why it matters ?

Digital sovereignty is often associated with technology sovereignty. The latter concept was broadly discussed in Europe in parallel with its loss in economic clout and with the increase competition in tech sectors. Chinese and US competition in high tech sectors challenge the capabilities of the EU to stay on the technology frontier. But talking about technology sovereignty is a larger concern than solely a question of competitiveness. First, it supposes that losing economic ground implies losing influence and geopolitical power. Second and reversely that the economic dominance in technology is not sufficient to entail technology sovereignty.

How digital sovereignty differ from technology sovereignty ? It is mostly a matter of the extent of technologies we are interested in. When we focus on digital we exclude other important frontier technology such as green technology and biotechnology for instance. Digital has to do with technology that transform, stock, transfer information whichever information is a signal, an image, an idea, a sound, words, figures...Some authors use alternatively digital and technology sovereignty. This is the case of Bauer & Erixon (2020) . But actually their definition is clearly bound to digital technology.

[1] In Guillou (2023), I also mention the libertarian philosophy which is at the roots of the digital economy and which inspires many of its leaders. There is then a broad tendency to consider the State as a barrier or as a competitor to rule the world.

Bauer & Erixon (2020) propose a definition of technology sovereignty through 4 dimensions: culture, control, competitiveness and cybersecurity. Culture refers to the consciousness that digital technology is used to manipulate information and determine the freedom of circulation and diffusion. EU felt it has specific values and market regulations which have to be protected because they are not shared by the rest of the world. Control is needed facing the tremendous financial and economic power of digital champions. Government have to control their abuse of power in terms of tax evasion, price policies, competition and technology use. The not-ending power of digital champions allowed by the economic model their growth is based on, challenge the State sovereignty. Competitiveness is basically the economic capability to compete in digital business based on digital technology. Cybersecurity refers to the control of the data flows used by digital businesses. Since digital technology create a virtual space where data flows have no frontiers, the classical sovereignty which uses physical frontiers to exert its police has to be renewed. It has to use new tools of control in order to respect the data property right, the integrity of information and prevent the weaponization of information to infer in domestic political issues. Given their definition, it is clear that technology sovereignty refers here to digital sovereignty.

Edler et al. (2023) attempt to define the digital sovereignty as a means to promote innovation.

Some digital technology are the pillars of digital sovereignty: IA, cloud computing, networks infrastructures, quantum computing, and semi-conductors. There are all highly connected and interdependant. Some skills are also necessary to ciment the State digital sovereignty: computing engineers, IA developpers, technical blue-collars.

In order to achieve a strong digital sovereignty, three attributes are necessary: a strong and innovative digital economy, large capabilities to master digital technologies and a set of laws and regulations to control and supervise the use and abuse of digital technology.

1.2 Assessing the size of the digital economy

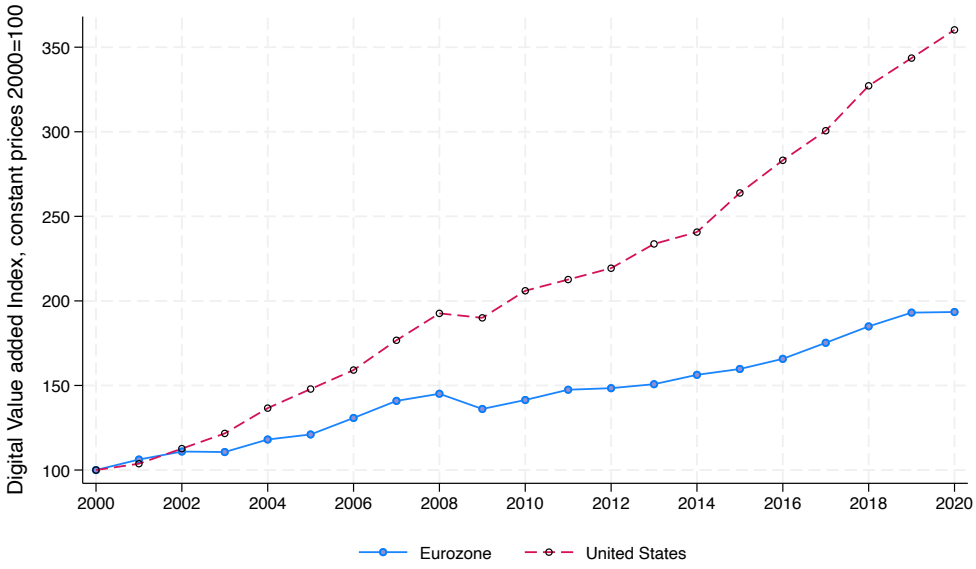
Nobody can deny that we experience a growing digital presence in Economies. But nevertheless, the measurement of the say presence is not as so easy.

If we measure the digital sector in terms of production, it does not constitute a very large portion of the wealth produced. For instance, in 2017, the share of the digital sector ranged between 4% and 10% of GDP in wealthy countries (Gaglio and Guillou, 2018; Guillou, 2020). Since digital activities cross sectoral boundaries, the actual share is likely somewhat larger. Moreover, this doesn't account for the deployment of digital activities in traditional industries (e-commerce, application deployment, etc.), which are not directly detected by a sectoral approach that focuses on the primary activity sector. Besides the actual production, we can look at other indicators to measure the presence of the digital economy in the contemporary economy: R&D expenditure, employment, profits, and capitalization.

In what follows we compare the United States to the Eurozone. The choice of the Eurozone instead of the European Union (EU 27) is first based on the availability of data and of the consistency of the monetary unit of account, second on the homogeneity of the zone in terms of technological advancement and institutional competencies.[2] The Eurozone represents 78% of the population,

[2]The Eurozone consists of 19 countries: France, Germany, Italy, Spain, Portugal, Ireland, Belgium, Luxembourg, Netherlands, Greece, Malta, Slovakia, Slovenia, Croatia, Cyprus, Estonia, Latvia, Lithuania, Finland.

Figure 1: Index of Digital economy value added, 2000 = 100



Source: EU KLEMS, 2024.

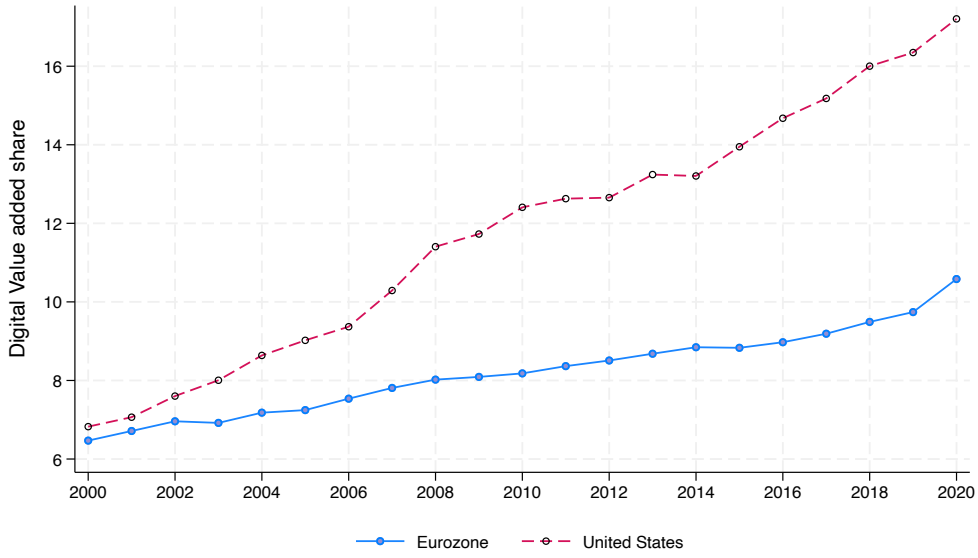
90% of the GDP and 87% of the R&D expenditure of the EU 27 respective amounts. Moreover, we will refer to the Eurozone as an economy.

The size of the digital economy is not directly retrieved from industry classification. It is indeed not a delimited sector with clear boundaries. Instead, digital economy has both a producer dimension as well as a user dimension. Regarding the producer dimension, some sectors can undoubtedly be named digital such as Information and Communication Technology (ICT) goods and services, or computer and software services, but some businesses belonging to traditional sector (Restaurant, health services, retail trade for instance) are provided through sophisticated internet platforms which undoubtedly make them actors of the digital economy and then digital sectors miss them. Nevertheless a first assessment based on the set of sectors which are bound to production of ICT goods and ICT services is rich in comparative results (see Gaglio & Guillou 2018).[3]

Indeed using data on value added at constant prices of ICT goods and services we can observe the 20 past years divergence in the position of the digital economy between the US and the Eurozone. First, Figure 1 shows the digital sectors value added index at constant prices: while the size of digital sectors in the United States went nearly fourfold, the Eurozone one weakly doubled. Of course, the growth rate of the total US economy was bigger than the Eurozone one, but the increase in the size of the digital sectors is also a result of its greater importance in the US economy over the 20 past years. Figure 2 shows that the share reached nearly 18% in the US though it reached 11% in the Eurozone.

[3]Using a 2-digit classification, digital sectors are then 26-27, Electronic, telecommunication and computer equipment, to which we add Information and Communication services from 58 to 63.

Figure 2: Share of digital economy relative to total business value added



It is broadly known that the US shelter big tech firms which recent growth was internationally tremendous. The so-called GAFAM for Google (now Alphabet), Amazon, Facebook (now Meta), Apple and Microsoft have been joined by AirBnB, Nvidia, Open AI, and have long been accompanied by the not so less famous Intel, Broadcom, Advanced Micro Devices, Oracle...

But it also stays important to assess how far the economy is digitalized since, as it was mentioned previously, more and more traditional sectors are increasingly leaning towards digital business and technology. One way to assess the digital user dimension lies on the analysis of the dynamics of investment in digital tools. More specifically, we focus on two types of assets: the ICT goods such as computer or telecommunication and electronics devices on the one hand, and the Software and Databases on the other hand. Evaluating software and Databases investment and ICT goods investment are another way of assessing how digital is the economy. But to scale it relative to the size of each economy we compute a ratio of investment per employee.

Investment in ICT good in the US is nearly three-fold the level reach in 2019 in the eurozone. When focusing on Software and databases, the divergence is not less striking while solely the double in the US. These results unveil that on average the digital capital at the disposal of one employee in the US is much more important, meaning undoubtedly that employment is much more digitized there and we estimate employment being on average 2.5 times more digitized.

When we consider the R&D expenditure of companies in the digital services sector ("IT services and software"), it represented 14% of the total global business expenditure in 2018 and 17% in 2020. These percentages are comparable to traditionally high contributors to R&D investment such as pharmaceuticals (18% in 2019, 19% in 2020), the automotive sector (15% in 2019, 14% in 2020), or technological equipment (computers and robots) (15% in 2020). The digital services sector, which accounted for 16% of the total in 2019, is thus just behind pharmaceuticals. This

Figure 3: Investment in ICT goods per employee

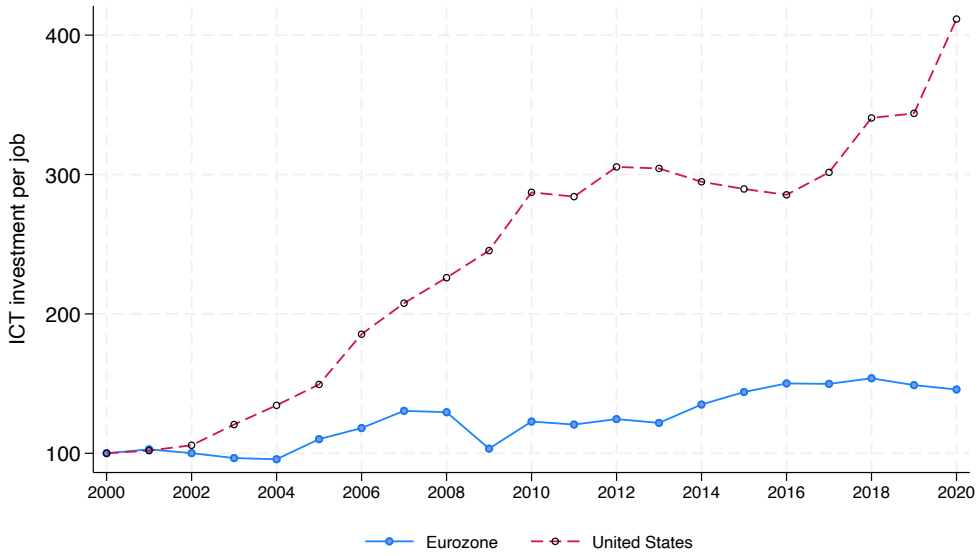
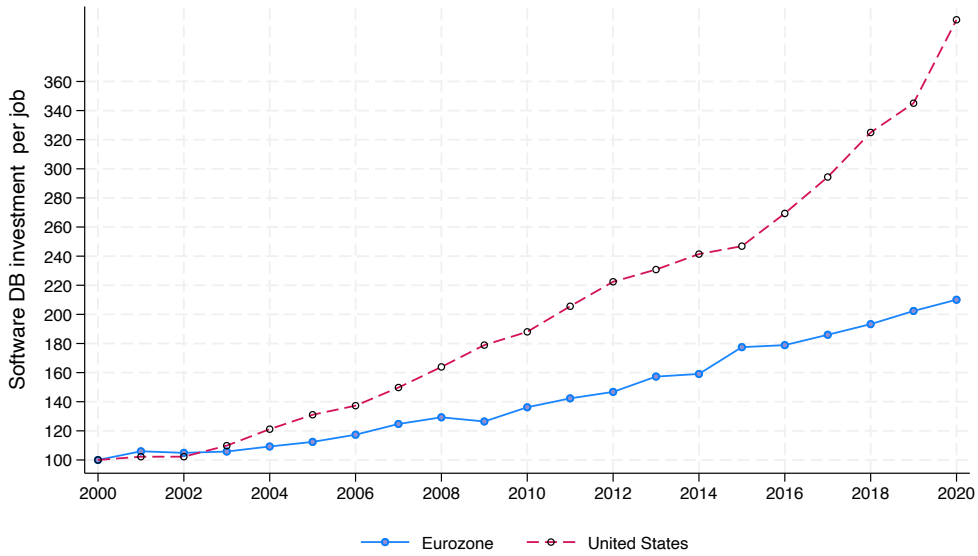


Figure 4: Investment in Software and Database per employee



position has significantly increased over the past decade. In 2012, this sector accounted for 4% of the total (i.e., $46 billion compared to $142 billion in 2020). The high percentage of expenditure is due to the massive research investment by the largest companies among them ($22.5 billion for Alphabet and $16.9 billion for Microsoft in 2020). Similarly, the presence of digital companies in this ranking (by number) was 9% in 2012 and 13% in 2020.

In terms of revenue, in 2021, Alphabet, Amazon, Meta, Apple, and Microsoft together accumulated $1.4 trillion in revenue. These companies have become conglomerates because they engage in very diverse activities. However, their revenues are often concentrated, meaning they come from a few of their activities. Apple derives most of its profits from the iPhone, Amazon from its cloud service (AWS), and Alphabet and Meta from advertising revenue, which is highly concentrated around a few advertisers. Additionally, application revenues are very significant for Alphabet and Apple, with very high margins since the maintenance cost is almost nil. For Amazon, marketplace revenues are increasing, as sellers pay 19% of their sales to use the platform, accounting for 22% of Amazon's revenue. Instagram greatly contributes to Meta's profitability through its marketplace revenues.

Finally, regarding capitalization, the UNCTAD (2021) report shows that the weight of digital companies in stock market indices' capitalization has continually increased. The capitalization of the top one hundred companies rose from $1.2 trillion in 2016 to $3.25 trillion in 2021, an increase of 170%. The CAC 40 index increased by nearly 60% over the same period. The report specifies that 68% of the capitalization of the 70 global platforms is American, 22% is Chinese, and 3.6% is European. At the beginning of 2021, only the European Deutsche Telekom was ranked among the top twenty global digital companies according to Forbes.

Another characteristic of these digital multinationals is their ability to expand into foreign markets without necessarily investing physically or deploying significant tangible assets. Their territorial presence is therefore less pronounced. This is particularly true for platform companies. Their growth model is primarily through the acquisition of other companies rather than creating greenfield capacity. Only e-commerce companies may engage in this type of investment due to logistics needs.

Revenues and capitalization significantly increased during the Covid-19 pandemic. This period benefited digital companies. A UNCTAD document studying the top one hundred multinational digital companies established that between 2016 and 2021, revenues increased an average of 23% per year, with a peak of 60% from 2020 to 2021. However, tech stocks are also very volatile and seem not to escape the economic downturn of 2022, which lowered their prices. The years 2020 and 2021 were prolific for these companies due to the concentration of consumption on their products and services. However, 2022 showed that there are limits to this seemingly endless growth. Firstly, the shortages of electronic components disrupted the value chains contributing to the production of these services and products. Secondly, having reached a certain maturity, these companies face a slowdown in consumption growth and a depletion of qualified workers and critical mineral resources.

New regulations (such as the Digital Markets Act in Europe) and decisions by competition authorities (particularly concerning commissions demanded for platform use or preferential positioning that platforms grant to their products and services) will also negatively affect their revenues. Despite a very dynamic market with frequent new entrants, the concentration process in the digital economy has been continuous.

1.3 Assessment of EU Digital Law

1.3.1 The needs for regulation

The digital economy is a very turbulent industry. Entry and exit are frequent thanks to fast innovation and obsolescence, but at the same time, given the huge scale effects of its economic model (high sunk costs, network effect and increasing returns), we observe a movement of concentration and the emergence of new monopolies powers.

Digital companies invest heavily in R&D to stay close to the technological frontier and pursue an omnivorous growth logic, diversifying more and more. They aim to aggregate related activities to create synergies. As Haskel & Westlake (2017) show, intangible assets, on which platform and digital activities are based, have the characteristic of creating synergies through aggregation.

The underlying business model leads to exponential growth, resulting in a very high concentration of economic power. Once the fixed cost is paid, the cost of serving an additional user is almost zero. Moreover, the more users there are, the more justified the use by others becomes, providing the company with a competitive advantage—known as the network effect. As the network grows, the cost of growth decreases. Here, the competitive advantage comes from both investments in innovation and the users themselves, especially if the company can capture them. Additionally, these companies have vast databases on consumers, their preferences, and habits, highlighting the formidable challenge of this concentration of power. For instance, Apple likely acquired UK-based Shazam to access all user musical preferences to enhance its streaming music platform. In September 2018, the European Commission approved this acquisition despite concerns about its impact on competing music platforms. Apple also acquired the magazine platform Texture, further increasing its service and user portfolio.

Online commerce is increasingly dominated by major platforms like Amazon and Alibaba. In the US, Amazon accounts for one in two online transactions and 75% of online book sales. When considering that these two e-commerce platforms are starting to buy traditional retail stores—Amazon acquiring Whole Foods, a high-end organic grocery chain, and Alibaba acquiring Intime, a shopping mall operator—their grip on retail seems limitless.

Some of these activities harm traditional industry competitors. This is the case with Amazon towards bookstores and publishers. Moreover, some actors like Uber are disrupting labor relations, challenging the rights associated with employment contracts. Resistance to these changes preceded concerns about market power, but the second concern can undoubtedly be fueled by the first.

The industrial organization of the digital sector increases the need for competition regulation and growing attention to the business models of these companies, especially their use of big data. Consumers or users can hardly make critical judgments, as the immediate gain—such as retailers using Amazon's platform, universities using Google's services, or artists using Apple's system to develop applications—is undeniable and lacks easy alternatives. It is up to regulators to protect them from future abuses of dominant positions. However, the regulatory path is delicate due to the sector's turbulence and dynamism. As long as new entrants challenge the rents of market leaders, the market functions well. When competitive or technological turbulence slows, regulators must carefully measure their interventions to avoid stifling market dynamics and provoking unfavorable asset relocations where rules apply. We are still far from international cooperation in this field, despite the market being clearly international.

Digital economy companies, especially platform economies, are keen on acquiring young innovative companies exploiting a technological niche. According to Affeldt & Kesler (2021), GAFAM acquired over 400 companies in the past ten years. Some large companies, in contrast, have more encompassing strategies, attempting vertical integration (like Amazon in distribution with the acquisition of Whole Foods) or diversifying into sectors where they want to apply their technological expertise: Google or Apple in automotive; Amazon or Google in medical or biotech. Notably, many traditional companies are digitizing and competing with platforms, such as Walmart, the largest American retail company, which acquired 75% of Indian e-commerce group Flipkart for $15 billion in May 2018.

Beyond the concentration of data-holding actors—dubbed the new oil by The Economist—online sales enable new associations and expressions of market power. Online sales allow for unconventional pricing, for example, through software that maintains artificially high prices. Specifically, digital cartels, agreeing on prices or quantities sold, can significantly harm consumers, as it becomes harder to detect these price or quantity agreements managed by such software. These programs calculate prices and quantities to market based on agreements among sellers, particularly concerning their margins. To be more concrete, think of online hotel bookings: the price adjusts to supply and demand and the time approaching the transaction. Such price-determination software also exists for airline tickets and on commercial platforms like Amazon. These price discrimination strategies approach perfect discrimination, where a company captures all consumer surplus, whereas in economic theory, when competition is fair, companies and consumers share the economic surplus.

Adding to these unconventional price and collusion strategies is a dense web of cross-participations in the same sector, making actors both competitors and partners. For instance, Uber holds shares in its main competitors such as Didi Chuxing (a Chinese ride-hailing service) and Lyft, while Didi holds shares in Uber. Many digital companies also invest in other digital firms. Apple, for example, has stakes in Didi. This portfolio diversification is also seen with digital investment funds. Japanese SoftBank Vision Fund has invested not only in Uber but also in its competitors Didi, Ola in India, Grab in Southeast Asia, and 99 in Brazil. In the private transport market, these cross-participations are a way of anticipating sector consolidation, as the dominance of a few global players or the coexistence of local players are both possible models.

There are also numerous cross-participations within the Chinese digital economy. The liquidity generated in these activities drives investments. Chinese companies are exemplary in this regard. Tencent holds stakes in Snap (10%), Tesla (5%), and Spotify. Tencent Music Entertainment and Spotify decided in December 2017 to buy each other's issued shares in a proportion below 10% of the capital to mutualize bargaining power with music labels. Tencent holds stakes in about fifteen foreign companies for $4.3 billion. Alibaba has also invested in foreign and domestic companies. Chinese digital firms have more freedom to invest abroad than companies in other sectors, although this freedom is increasingly constrained. These investments are strategic, creating positive externalities for the company by bringing new customer networks, complementary uses, or entries into foreign markets.

Ultimately, these cross-participations signal a concentration of shareholders in digital companies, potentially leading to faster and more immediate economic concentration.

Thus, concentration in many respects in the digital industry is a structural trend, erecting a power of influence, control of large information pan, and market structuring that threatens the economic sovereignty of states. Moreover, exercising state counter-power requires digital technical skills often

lacking in government agencies, which then resort to consulting firms for IT or digital services. The regulator's task is significant, demanding constant effort and responsiveness, especially when these private powers touch on sovereign missions.

1.3.2 The EU digital legal arsenal

A large series of Acts have been voted during the 4 last years which provides the EU with the capabilities to control and secure digital flows of data and information. General Protection Data Regulation are a set a rules which changed a lot our access to internet website since it obliged any website, even non commercial sites, to warn about the use of the data of the platform's user. The GDPR came into effect in 2018. The philosophy behind the regulation is to ensure the protection of users' and citizens' data from third-party usage. One of the fundamental principles to ensure this protection is the territorialization of the data used. The regulation does not prohibit the transfer of data outside the European territory but conditions such transfers to restrictive reciprocity conditions. The EU maintains a list of countries – currently narrow – that meet these conditions, effectively requiring these countries to have adopted legislation equivalent to the GDPR. Otherwise, data transfer is possible if the company using the data complies with security rules defined by the EU and if the user's consent for the transfer has been obtained after complete information about the transfer and if the transfer is essential. These rules apply to all companies offering their services to European residents, whether or not they have infrastructure or legal entities within the European territory.

Then came the Digital Markets Act and the Digital Services Act. The Digital Markets Act (October 12, 2022) and the Digital Services Act (October 22, 2022) establish rules for fair competition among digital players and platform operations. The first intends to regulate the markets in order to supervise concentration and the creation of unfair and detrimental dominant position. The second intends to regulate the services provided by the business platforms in order to respect data property and to control abuse of power detrimental to consumers.

Still pending are the talks around the cybersecurity Act and the constraints to put on cloud computing providers: the EU Cloud services proposal lists the requirements demanded to the cloud computing providers in terms of transparency, security, location of infrastructure and origins of capital. But so far (June 2024), disagreements among EU members led to the return to less demanding version of the law discarding the French SecNumCloud standard

In Guillou, G'Sell & Lechevalier (2024), we show the large and complex EU debates around the cloud computing regulation and the different position of members relative to technical requirements in order to increase EU digital sovereignty.

All in all, these acts are undoubtedly an EU soft power because it creates judicial expertise which can inspire a lot of less advanced countries.

European regulation can be seen both as an obstacle and a substitute for the development of powerful digital players. The GDPR undermines the accumulation of user data from third parties like advertisers and content publishers and may deter the creation of applications in Europe based on such data accumulation. Meanwhile, companies like Alphabet and Amazon already possess such extensive data accumulations. European entrants face constraints that did not exist during the early development of American digital giants.

Regulation also creates opportunities for new security services that will later be demanded by

non-European actors. The EU is betting on the importance of its user market, whose size undeniably forces compliance with European rules. Legal dominance could turn into economic advantages for companies that comply with the rules first.

The question of whether European law would have been different if there had been more European digital champions is not simple to answer. Considering the automotive industry, a major sector in Europe, regulations have not been significantly hindered. The lobbying by these companies has likely been non-neutral but not more pronounced than the lobbying by American digital companies.

The absence of digital champions is problematic in unexpected areas. A significant part of digital power is built within regulatory industry committees. This is where technological standards and norms are decided, exerting major influence on the industrial trajectories of companies and their competitiveness.

The main international standardization bodies are the World Wide Web Consortium (W3C), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunication Union (ITU). The latter is a UN agency for the development of information and communication technologies. Its Secretary-General, Houlin Zhao, is Chinese. In 2020, the EU has more influence in the ISO and IEC bodies than the United States or China but is less influential in the ITU or W3C.

1.3.3 The EU legal activism

So far, competition authorities' control over digital companies has primarily come from the European Union, notably against Microsoft and then Alphabet for using their software and search engine to promote their products and services, thus hindering competitors in those niches. This led to an initial fine of €497 million for Microsoft in 2004.

For Alphabet, due to search engine manipulations to favor its own online shopping site—Google Shopping—over competitors, the European Commission imposed a €2.42 billion fine in 2017 for the damage caused. Additionally, on July 18, 2018, after more than three years of investigation, European competition authorities fined Google €4.34 billion for abusing its dominant position. The accusation was that Google abused the dominance of its Android operating system by imposing default installation of its applications, particularly its search engine, on mobile phone and tablet manufacturers. Google argued that this was the counterpart for providing its operating system for free and allowed for the return on investments made in it. This growth model—offering services for free to acquire a critical mass of consumers for advertising and consumer data—was Google's defense. Google appealed these decisions but lost. This decision satisfied its European competitor, the French search engine Qwant, though it did not compensate for the market share losses Qwant likely suffered from Google's practices. Qwant is part of the Open Internet Project association, which was a plaintiff in the Google case. Then, on March 20, 2019, the Commission imposed a third fine for abuse of dominant position concerning Google's advertising business AdSense. The amount was €1.49 billion, representing less than 2% of 2018 revenue. Google was accused of imposing AdSense for advertising, creating unfair conditions for its competitors, such as the French company Criteo.

In June 2021, the French Competition Authority fined Google €220 million for abuse of dominant position in the online advertising market. This fine is relatively small compared to the $147 billion in advertising revenue, but it is a decision that will lead to some changes in Google's behavior.

The European Commission followed up by opening an investigation on June 22, 2021, into Google's practices in the advertising market.

Spotify also filed a complaint against Apple for abuse of dominant position. Despite being a leader in the online music market, the Swedish company faces growing competition from Apple and Amazon. Spotify accuses Apple of abusing its dominance in the app market with the App Store to impose its music app and having to bear a 30% commission to offer its music platform via the Apple Store payment system. Apple argues that Spotify uses its marketplace and should pay for it. The online gaming company Epic Games also sued Apple over the terms of use of the Apple Store (particularly the 30% commission). Apple faces class-action lawsuits from a group of app developers. While the company has conceded some fee reductions for small developers and allowed tariff communications outside the app, it refuses to host other app marketplaces on its devices and insists that purchases go through its payment system. The "Coalition for App Fairness", which includes Epic Games (the publisher of Fortnite) and Spotify, contests this model. In the US, Epic Games' complaint did not succeed, and it was ruled on September 10, 2021, that Apple did not violate antitrust laws. However, the appeal of January 2022 of the May 2021 decision is expected to be more challenging for Apple, as third parties, including the Department of Justice and Microsoft, have joined.

Competition authorities worldwide are increasingly mobilizing against these companies following the European authorities' lead. In the US, in early June 2019, the Department of Justice (DoJ) and the Federal Trade Commission (FTC) decided to investigate giants Apple, Amazon, Facebook, and Google, while the House of Representatives also tasked a committee to investigate the monopoly powers of these same companies.

The specific problem with GAFAM is that their market power does not explicitly result in higher prices, making it difficult to establish the existence of monopoly power. Lina Khan (2017) proposes separating infrastructure (platforms) from their exploitation (commerce), similar to how railroad monopolies were once treated. Lina Khan, a law professor at Columbia University and appointed head of the FTC since 2021, emphasizes that controlling both the platform and the goods and services sold on it creates an abuse of dominant position that hinders the growth of competitors. This is the case, as seen with Spotify, the online music service competing with Apple Music. It's also the case with Google, which prioritizes its own products in its search engine, or Amazon, which ranks its own products first and uses data collected from its competitors. The entry of new players against these giants becomes increasingly risky, a risk even recognized by investors.

From the perspective of innovation and the end consumer, these companies are almost beyond reproach. Generally, they have relatively low margins, distribute few dividends, invest heavily in R&D, and price their products quite low or even offer services for free. Competition authorities, concerned with consumer welfare, have little to criticize. The question is whether their size will harm consumers in terms of price or product quality in the future.

Some competition economists now talk about a "data-gopole." Facebook is the archetype of this data monopoly, and it's almost a relief that the company is banned in China. Despite the highly publicized Cambridge Analytica scandal, it had no impact on its user numbers. Knowledge of these users is a goldmine for politicians and advertisers, and advertisements are the primary revenue source for platforms. Google and Facebook capture almost 75% of online advertising spending in the United States. Advertising revenue constitutes a major portion of Alphabet's (via Google) and Meta's (via Facebook) income.

The EU regulator's actions have been significant, demanding constant effort and responsiveness. It is all the more essential especially when these private powers touch on sovereign missions.

Section 2. The Regalian Missions

If states are increasingly on guard against digital giants, as observed in China, Europe, and the United States since 2020, it's also because they threaten their sovereign missions. Here we will discuss, on one hand, the control of currency and means of payment, and on the other, cloud services and security, where dependence on giants vies with their instrumentalization by states themselves.

2.1 Currency and Finance

Some multinational corporations reached market capitalizations and activity levels which surpass the wealth or GDP of certain nations. Their liquidity levels are sometimes such that their interventions in bond markets can be significant. Financially, some of them exceed the balance sheets of certain central banks (Hyppolite and Michon, 2018).

When Facebook (now Meta) decided to create a digital currency in 2019, named Libra, no one believed it was technically impossible, but the existing banking system clearly opposed it. To this day, banking regulations remain very stringent. Yet, the idea of creating a "stable coin" was not revolutionary, as other stable cryptocurrencies (backed by reserves of crypto assets or legal tender currencies) already existed. However, the project was more ambitious and relied on a user network constituting an unparalleled leverage in Fintech, with backing from a basket of currencies. Regulators, clearly concerned about this project, managed to dissuade major partners like PayPal or Visa, then the members of the Diem consortium tasked with carrying out the project. In addition to regulators, government representatives have shown great hostility. For example, Bruno Le Maire expressed opposition by stating that "the monetary sovereignty of states [was] at stake". Nevertheless, it was the American authorities who showed the most resistance. In February 2022, Facebook abandoned its digital currency project. One of the concerns was the use of financial data made accessible to the platform and its potential overlap with data from the social network (even if this was excluded in principle). With over 2.85 billion users, Facebook would have had a considerable sales force for its financial services. Despite this failure, the project was recycled into a less ambitious version of a digital currency allowing transactions between users on the various platforms managed by Meta.

In the absence of being currency issuers, their ability to create means of payment and credit is not a technical challenge but a regulatory one. In China, it is also regulatory power that has set limits on digital giants like Alibaba. Until 2019, 90% of digital payments were made through Alipay or Tenpay.

It's worth noting that an institution offering credit creates money by default. A nebula of companies is emerging in Fintech that constantly challenges the centralization of monetary creation and banking regulations. Central banks have understood that they must also invest in digital currencies. A survey showed that 80% of them had begun to study the subject, although they are proceeding in this area with great caution. In 2020, the Bank for International Settlements

(the central bank of central banks and the regulatory authority) published a report on central bank digital currencies. This report outlines the main challenges associated with the creation of central bank digital currency while indicating that it will be difficult to avoid the emergence of this additional means of payment. Although a central bank digital currency would have the particularity of having reserves as counterparts in central bank accounts, the challenge is monetary and financial stability. The report acknowledges the advantages of such a currency in parallel with the growth of economic transactions conducted digitally and the globalization of exchanges. A digital currency would facilitate exchanges in the global space while guaranteeing stable and secure value. The greatest risks to be addressed are the risk of hacking and cybercrime, and the drying up of deposits from second-tier banks that would lose their power of monetary creation. The first risk requires security and encryption protocols that can slow down the fluidity of using such a currency and thus affect its main advantage. The second risk involves a partial transfer of credit issuance, and thus monetary creation, to the central bank directly or to issuing digital services that would be authorized to open lines of credit in this currency to sell their goods and services. The advantage is the elimination of an intermediary while maintaining control of the money supply; consumer credit would be governed by private digital actors. Only investment credit would remain within the realm of traditional currency, but for how long? Thus, central banks are far from reaching a conclusion on this matter. The collapse of cryptocurrency values in 2022 gave them some respite, as it was these cryptocurrencies that had prompted them to accelerate their deliberations.

The main cryptocurrency, as mentioned earlier, Bitcoin, was created in 2009 by Satoshi Nakamoto, a pseudonym. Its value has seen highs (for example, $70,000 in November 2021) and lows (less than $20,000 in June 2022), but its number of users has continuously increased until the crash of winter 2022. Bitcoin, like other cryptocurrencies, is based on blockchain technology. The nebula of Fintechs using cryptocurrencies has greatly densified over the past decade. Among them, Binance, a cryptocurrency trading platform, is the archetype of a multinational corporation without nationality and defying regulations.

Crypto assets are becoming increasingly popular, but to date, they finance only a small part of the official economy. Among them, stable coins have attempted to counter volatility, the main drawback of cryptocurrencies. These stable coins stabilize the value of the crypto portfolio by approaching the traditional monetary system. They serve as currency vehicles in cryptocurrency markets. There are a large number of stable coins, but the three most important ones are USDT (tether), USDC, and BUSD. Their value is backed by assets in dollars (deposits or bonds), other fiat currencies, over-collateralized crypto asset reserves, or is based on an algorithm, as was the case with Terra (UST) which collapsed in 2022. The foreseeable tightening of monetary policy (increasing interest rates that dry up available liquidity) and regulation, as well as China's ban on mining, destabilized the market. The collapse of Terra and its counterpart Luna followed position liquidations caused by market reversal anticipations, while Terra's valuation structure was considered too weak. This collapse showed the fragility of the crypto asset market, still very open to very risky, if not fraudulent, experiments and setups, as demonstrated by the liquidation of the FTX trading platform in November 2022.

However, the proliferation of stable coins (digital currencies not issued by central banks) remains a challenge to monetary policy. They seek to offer a monetary dimension to cryptocurrencies, but they do not fulfill all the functions of legal tender currencies: they are not bound by borders and seek to circumvent the rules specific to financial institutions. Regulating a stable coin requires

international cooperation.

Some commercial banks indicate that they wish to adapt to changes and are willing to invest in a digital currency for their clients, a digital currency that would put them in direct contact. This is the case, for example, with JP Morgan, which is working on such a subject. Although seemingly losers at first glance, as no intermediary fees would be collected, private banks cannot be completely ousted from this new means of payment. If JP Morgan managed to implement such a system, it would mean the establishment of a decentralized and parallel payment system.

On the other hand, the European Central Bank launched the testing phase of its central bank digital currency in July 2022. This phase will last for 24 months during which the level of ....

2.2 The Cloud or Digital Archives

Public archives of personal data and historical documents are most often managed by the government for at least two reasons. The first is that they are a public good that benefits everyone, and while the consumption of this good by one person does not diminish its service or quality for others, no individual will want to pay the price for it if it benefits everyone. The second reason is that this data often has a critical and confidential nature (such as health data and foreign policy archives), which requires a transcendent, impartial, and responsible authority for the integrity and inviolability of this data.

However, the archiving and storage of data are now digitized processes that require digital infrastructures and software to operate these infrastructures. The purpose of archiving is to provide ordered information when requested. Digital storage services, a mission of cloud services, are primarily provided by American actors such as Microsoft's Azure, Amazon's AWS, and Google's GCP (Alphabet). Today, these three actors own more than half of the large-scale data centers (hyperscale). Amazon and Microsoft generate more than half of the revenue from digital storage and processing services worldwide.

While some large companies have their own data storage infrastructure, they increasingly rely on external data centers that offer archiving and processing services. However, there is also a trend towards fragmentation of services to meet the proximity needs of connected objects communication.

There are indeed European actors—French OVH ranks seventh globally—but they struggle to secure large public contracts. Most of the data from large public bodies is usually archived by American operators.

The increasing digitization of public services also leads to the generation of numerous data, part of which will be archived and require computational data processing services. Apart from defense, most ministries use external providers to store, organize, and process data associated with the operation of their services. Data storage infrastructures are expensive and require new technical skills not always available within administrations.

This activity of archiving and processing citizen data, which was once done internally through non-digital means, is now outsourced outside the service. Undoubtedly, digitization has greatly increased the efficiency of public governance, but outsourcing data storage and processing increases the risks of disclosure and non-compliance with information ownership. The risk increases when storage is done by a foreign provider, or even abroad, and respect for ownership and confidentiality depends on foreign laws. We will return later to the specific problem of American law.

To address the absence of European actors and face American dominance, French and German authorities have created a label required to host the most sensitive public data, the SecNumCloud label. This label, based on the ISO 27001 standard, was established in December 2016. Defined by ANSSI in France, it details the characteristics that a cloud service must meet to ensure security requirements regarding the respect of ownership and confidentiality and the security level against cyberattacks. In theory, this label constrains bidders for public contracts. Moreover, the government has specified, through successive circulars, the doctrine for purchasing cloud services, which has been synthesized in the "Trusted Cloud" doctrine.

In parallel, France, but also Europe, has initiated an industrial policy to support the cloud sector. In November 2021, the French government implemented a support plan for the sector worth €1.8 billion over four years, with €667 billion in public financing from the French state. The Important Common European Interest (IPCEI) project for cloud research was launched in December 2020. Furthermore, the European project GaiaX tries to counter American dominance by creating a set of technical interoperability rules to increase access to these services for European companies.

GaiaX originated from a French-German initiative in 2019 establishing an organization tasked with federating cloud services that would comply with a specification in accordance with the General Data Protection Regulation (GDPR) and offer interoperable services to allow more flexibility in using data center services. The organization was taken over by the EU to facilitate European actors' access to efficient cloud infrastructures that comply with European rules. GaiaX has been the subject of recurring criticisms, notably due to its open approach, which allowed major American market players to become members and crush weaker European competition. Undoubtedly, the project had a functional basis and was not the vector of a policy to create a European cloud. It was about allowing European companies easy access to a tool increasingly critical for the development of the Internet of Things or the use of artificial intelligence to optimize economic activities.

Here we find the legalistic and competition-respecting approach of the EU, which does not spontaneously resort to industrial policy to solve the problem of insufficient European supply and seeks primarily to federate European companies around a unified service. The strategy of creating a European champion is therefore abandoned at this stage. France already had an unsuccessful experience with the companies NumEnergy and CloudWatt, short-lived French cloud actors supported by the state from 2012 to 2015 before their respective closures in 2018 and 2019.

While this may be regrettable, it must be acknowledged that the European legalistic position is quite tenacious and influential. In the digital field, the past five years have been prolific. The General Data Protection Regulation (GDPR) came into force in 2018. It was followed by the Digital Markets Act, then by the Digital Services Act. Legal decisions have invalidated data transfer agreements with the United States. A digital data and market law has therefore been developed, which constrains digital services, including cloud services.

These projects, like GaiaX, demonstrate the mobilization of public authorities around the issue of digital services and legal and security risks. The intertwining of regulations and projects is complex, not to mention regulatory bodies. However, the lesson from the past decade of cloud policies (2012-2022) shows that the regulatory dimension (thus technical and legal) is fundamental, and the scalability effect that European actors can hope for requires first the regulatory integration of the European market, which took shape relatively late.

Nevertheless, political will sometimes contradicts political principles, either out of pragmatism or lack of courage. The case of health data in France shows how difficult it is to reverse the advantage

gained by hyperscalers. Indeed, it was decided in 2019 that the data from the Health Data Hub, the French health data platform, would be hosted by Microsoft (Azure service). Eventually, concerns about the extraterritoriality of American law led to the desire to redirect this data to a French provider. At the beginning of 2023, the migration decision had not yet been announced or made, nor had the choice of the new French or European host been announced. The question of the territorialization of data storage centers remains at the heart of digital sovereignty. We will return to this later.

2.3 Communications and Surveillance

Communications and Surveillance Information is a strategic asset for governments. Indeed, it is a key asset for surveillance purposes to maintain law and order, security, and ultimately for the military defense of the territory. To obtain information, communication and information collection networks are the physical infrastructures that require particular attention from governments. As Nathaniel Persily (2022) shows, the Internet has provided unprecedented means for states to control their population and serve authoritarian tendencies.

Today, this requires mastery of three spaces: terrestrial and underwater space firstly with the telecommunications infrastructure deployed there; extraterrestrial space, from low orbits to high orbits of navigation and geolocation systems; and finally, virtual space, or cyberspace, the boundaries and property rights of which require legal innovations.

Digital communication infrastructures are increasingly extensive on land and at sea. While undersea cables are indeed power and control stakes for Internet flows, it is terrestrial telecommunications infrastructures that have been intensely crystallized around sovereignty issues, particularly concerning the activities of the Chinese company Huawei.

For the record, Huawei, founded in 1987, was in 2020 the largest telecommunications equipment supplier, with revenues of $105 billion and employing 80,000 researchers. To grow, the company has heavily invested in R&D and the employment of engineers and researchers. In 2020, according to the global ranking of the 2500 largest R&D investors (EU scoreboard, 2021), Huawei was the top Chinese and the second global company with €17 billion (surpassed by Alphabet with €22 billion in investment, while Nokia and Ericsson's R&D investments reached €3.8 billion). The company holds 87,000 patents and over 1,400 patent families in 5G (compared to 1,427 for Nokia and 827 for Ericsson). It employs 12,000 people in Europe (out of nearly 200,000 worldwide), which is its second-largest market after China, and achieved approximately a quarter of its total revenue in Europe (€111 billion in 2020). In 2019, it had 40 contracts related to 5G equipment with foreign countries, half of which were in Europe and the rest in Asia (Singapore, Thailand, Philippines, Malaysia, Indonesia).

When Huawei arrived in Europe in the early 2000s, telecom operators seized the opportunity of this low-cost supplier. Huawei would be accused of intellectual property theft and dumping, but it continued its progression, putting other suppliers in difficulty, such as the British Marconi, which was the supplier of British Telecom and was then acquired by Ericsson in October 2005. Nokia and Ericsson then sought to involve European authorities to counter Huawei's dumping made possible by Chinese government export subsidies. Huawei's penetration into Europe was hampered by suspicions of espionage toward the company, which is closely tied to the Chinese government, and by US accusations. Even Poland, very welcoming to Chinese investors, did not hesitate to

prosecute a Huawei employee accused of espionage. Under high surveillance since 2012 for security reasons, the US Department of Justice accused it of intellectual property theft in January 2019, then in May 2019, the US administration decided to give the Department of Commerce the right to ban certain electronic component transactions. While the text does not expressly target Huawei, the target is obvious and will lead Huawei to accelerate its chip production autonomy strategy. However, contracting with over 250 American suppliers, especially in chip design, the ban is a real threat to the company. The threat materialized under the Joe Biden administration when the Department of Telecommunications decided to ban Huawei (and the other equipment supplier ZTE) from selling their equipment in the United States for national security reasons.

The serious question that other governments are facing today is: Can Huawei use its equipment to create means of espionage for the Chinese government? Its owner and leader, Zhengfei Ren, denies such intentions in the media, but the problem comes from the Chinese government's policy, which does not hide its ability to demand companies' cooperation for established party interests: the Chinese government blocks Google and Facebook in the name of domestic security. On their side, the United States have not always been neutral and may have solicited private companies like Cisco to participate in intelligence operations (according to Edward Snowden's revelations).

In Europe, Huawei is mainly present in the United Kingdom, in the 3G and 4G networks, but has been subjected to serious technical controls. The 5G technology poses more security challenges because it is expected to be deployed in various devices (automobiles, enterprise equipment, daily consumer objects) that will transmit data. At the beginning of 2019, the German, French, and Czech governments put a brake on Huawei's 5G deployment. Deutsche Telekom reconsidered its partnership, and Oxford University suspended donations and scholarships from the company. The German government, which was supposed to launch the first 5G auctions in spring 2019, hardened its stance towards Huawei, although it did not completely exclude it. On the other hand, in the United Kingdom, the reluctance caused by American pressure, coupled with information sharing by the NSA (National Security Agency), was overcome, and the British cybersecurity commission deemed it could manage the risk. Ultimately, Boris Johnson reversed Theresa May's government authorization in July 2020 by banning Huawei from British infrastructure and requiring its removal by the end of the year for new purchases and by 2027 for installed equipment.

While Monaco Telecom (55% owned by Xavier Niel, the CEO of Free) has contracted with the Chinese operator for the deployment of 5G, Italy should not remain closed to this operator given its participation in China's Belt and Road Initiative, although these two rationales are disconnected. Therefore, it will be difficult to maintain a common front against the Chinese operator in Europe.

In 2020, the EU published a document establishing the security measures necessary for the adoption of 5G technologies. This document urges member countries to verify if their 5G deployment plans meet security requirements and to implement what is necessary to comply. This is crucial for the security of communication infrastructures in Europe. Some see these recommendations as obstacles to the rapid adoption of 5G in Europe, given the competitiveness of Huawei's offerings compared to those of Nokia and Ericsson. This highlights the trade-off between competitiveness and sovereignty.

2.4 Space Communication

At the extraterrestrial level, full mastery of space is concentrated in the hands of Europe, the United States, and China. The latter has made enormous efforts to catch up with the other two. It completed its satellite navigation system, Beidou, with the launch of its 55th satellite in 2020. The project started in 1994, with the first launch in 2000. The project obviously had a military foundation and experienced accelerations in reaction to geopolitical crises. Hillman (2021) specifies that the Chinese sought and obtained assistance from American companies such as Loral Space and Communications and Hughes Electronics Corporation. These companies were then sanctioned in 1999, and control over exports related to space conquest was reinforced. The Europeans were more open since they allowed Chinese actors to cooperate in the construction of Galileo, with funding of $228 million, but the Europeans remain owners of the hardware and intellectual property.

Unlike industries like solar panels or batteries, China is far from independent in space and aeronautics and imports many components and technologies. Although seemingly infinite in dimension, extraterrestrial space accessible with 21st-century technology is soon to pose questions of appropriation competition, particularly because some orbits are almost saturated. While communication satellites can be private, the allocation of emission spectra remains a prerogative of states. Companies must obtain emission spectra from the International Telecommunication Union (ITU) and ensure compliance with the legal constraints of the territories to which they transmit. In China and Europe, space communications are dominated by public actors. In the United States, private actors are increasingly present, and it is not insignificant that digital giants and platforms are found there.

SpaceX was launched by Elon Musk and stands out from other private actors like Google or Amazon. Once considered fanciful, SpaceX now conducts two-thirds of NASA launches. Thanks to its reusable rockets, the company has reduced launch costs by three, which now amount to $62 million, and promises further cost reductions. SpaceX also plans to deploy a constellation in low Earth orbit to make the Internet accessible to the most remote areas. Elon Musk's first Starlink constellation was launched in 2019 and aims to have more than 12,000 satellites by 2027. The goal is to make the Internet accessible everywhere in the world, especially for long-distance communications and users in remote areas without terrestrial infrastructure.

Amazon (Kuiper), Meta (PointView LCC), and Alphabet (Loon) also have projects to launch constellations in low Earth orbit. Little is known about the first two. Google chose to forego satellites but uses balloons launched into the stratosphere and inflated with solar energy, which act as relay antennas in the sky. Google has faced political opposition, seeing these balloons as a means of surveillance by Americans.

The mission of reducing inequalities in Internet access is clearly stated by these companies. It must be said that these projects to deploy the Internet in poor areas are hardly profitable, just like low Earth orbit constellations in general. Bankruptcies are numerous (see the cases of Iridium, Intelsat, and OneWeb bailed out by the British government, in Chapter 4). It is therefore more of a means than an end. For Musk, the ultimate goal is the colonization of the planet Mars.

The deployment in low Earth orbits for the purpose of universalizing Internet service is a geopolitical weapon that only China has kept under its control, with the United States and Europe entrusting such activity to private actors. However, according to Hillman (2021), providing Internet services to remote regions of poor countries is a launching pad for other economic and political cooperation.

On its side, the Chinese government created a state-owned enterprise responsible for communi-

cation satellites, China Satellite Network Group, in 2021, and notably plans to launch a constellation of 12,000 satellites into low Earth orbit. Profitability is not the priority. Chinese delays could turn into an advantage if public financing allows the conquest of markets abandoned for profitability reasons. Once again, China seems to have found ways to consolidate its economic sovereignty by controlling the economy of its partners and subsidizing its imperialism.

Space surveillance is part of its defense and security policy and control of its population. From facial recognition technologies to reasoned territorial mesh, the alliance of artificial intelligence, crowd and aggressor psychology, and numerous spatial data will provide additional means to the Chinese security forces for maintaining order.

For all countries, the security mission is no longer just about the physical integrity of the territory and people; it increasingly concerns cyberspace and respecting the integrity of citizens' and companies' personal data that transit through networks, as well as all attacks on public infrastructure by digital tools.

Section 3. What could be done to improve the strength of the EU digital sovereignty?

In this section, we present the three most important trade-offs that the European policy-makers are facing to design policies in order to improve the strength of the EU digital sovereignty. Then we highlight some guidelines for the design of policies and the necessity to stick to Europe principles : protect the integrity of information which is a pillar of European institutions, protect the competition and keep fighting against the abuse of dominant position and feed the scientific and enlightment legacy of the continent through a massive investment in education.

3.1 The intractable dilemma

We present the three most important trade-offs that the European policy-makers are facing to design policies in order to improve the strength of the EU digital sovereignty. The first is a matter of time: short-term competitiveness versus long-term sovereignty. The second is a trade-off between consumer and companies when the matter of data integrity and protection is in question (Janßen et al. 2022). The third is a trade-off between competition and protection to boost innovation when learning and scale effects are at play (Nicoletti et al. 2023, Gal & Aviv 2020).

The first trade-off results from the nature of digital technology. They are general-purpose technology that can be used well over the digital companies themselves. These technologies are needed to boost growth and to provide the means to innovate in other sectors such as pharmaceutics or agriculture for instance. There are also needed to improve the public services that the administration provides and in general the state governance. But the lack of local providers or their too small size create a dilemma when the State wants to cherish them in order to augment their size. The demand from the private sector is as well directed to the dominant players feeding their dominancy and market share. The abuse of dominant power can be under the control of the competition authority but it is hard to control the abuse when the monopoly does not affect an empty competition.

The second trade-off faced by policy-makers is the opposition of interests between end-consumers and firms when the matter is data protection. Indeed strong privacy laws and data protection are good for users but are an additional cost for companies. The question whether consumer protection prevents firms to innovate is not easy to demonstrate. However companies have to adapt to complex regulation and adjust their production. The regulatory constraint is the same for all companies on the territory where the law is implemented but innovation has no frontier. A high level of regulation can divert the place of innovation to countries with softer legislation.

The third trade-off is between protection and competition. This is related to the first one. Digital players need to reach as soon as possible an efficient scale to be profitable and capable of investing in future research to keep up being on the technology frontier. Competition is the best way to allow entries of new comers and to motivate investment to improve products and process. But if competition is too harsh, getting an efficient size is out of reach. This is the classical problem of the infant industry. Protection may be necessary to help the firm to start and become sufficiently competitive to face international competition. But protection is for existing firms not the ones to come. And protection has to be ended finally (Greenwald & Stiglitz 2006). Technological protectionism is more and more prevalent among trade policies of protection. This international context of protection policies triggers retaliation measures and complexifies the trade-off because now protection is also motivated by geopolitics. Such a protectionism could bring a threat of moral isolationism (Shelley-Egan & Vermaas 2024) which is, in a long run, bad for scientific and technical progress.

3.2 The design of policies

To boost the digital economy's size, the EU policies should change the scale, the focus and motivate the entries.

The US digital economy dwarfs the EU one as shown by statistical evidence. Many reasons have been put forward to explain that the EU started too late in the digital competition and was outstripped in many digital markets. The industrial history of the EU is one of them as well as an unsufficient taste for the risks of its entrepreneurs and investors. It is then not only a question of bad policies. Not more it is only policies that could reverse the position of the EU in the race. But nevertheless, given the importance we've just underlined of the digital sovereignty, it is crucial to design policies which could enhance this sovereignty. For what concerns the digital economy, it is striking to observe how far the level of investment is lagging behind in Europe. In AI, Europen Court of Auditors (2024)'s recent report points the shortfall in investment compared to the ambition of the EU commission.

The financial resources deployed by recent national and European plans do not seem entirely commensurate with the challenges. These challenges can be evaluated using technological metrics. Whether it concerns patents in breakthrough innovations (UNCTAD 2023, Bellit & Charlet 2023), scientific publications, the number of companies among the world's leading R&D investors, investments in ICT or intangible assets, the European Union is deviating from the trajectory of the United States and is being closely followed by China in many technologies. For instance, Guillou, Bock, Elewa, Nesta, Napoletano, Salies & Treibich (2024) show the gap in investment between the US and the eurozone. The smaller growth in labor productivity in the eurozone relative to the US over the past 20 years turns to be the main culprit of the smaller growth in GDP per capita of the

former. Assuming the employment volume remains unchanged on both sides of the Atlantic and the United States maintains its capital intensity, over the next five years of the European mandate, approximately an additional €260 billion would need to be invested in ICT to match the American investment per job. In terms of R&D, an additional annual investment of €313 billion would be required to equal the average volume of R&D per job in the United States. This amounts to a total effort of 4% of the Eurozone's GDP.

This gap in capital intensity partly explains why the European Union's GDP per capita is lagging behind that of the United States due to significantly slower productivity gains, hindering its ability to absorb major cyclical shocks, notably the energy shock. We can find evidence in Bock et al. (2024) that the rapid growth in the US investment in ICT goods, R&D and Software and database was mostly driven by high tech services and specifically ICT services, among which we find the big digital US champions.

If we sum up all the IPCEIs since 2018, we reach a total of €27.75 billion in public funding, which is expected to be supplemented by approximately €50 billion in private investment. Additionally, there are funds from NGEU amounting to €750 billion. Over five years, this total of approximately €828 billion seems to address the investment challenges for the next five years, particularly necessary for the energy transition (€150 billion per year according to Mafhouz & Pisani-Ferry 2023) and artificial intelligence (€150 billion per year according to Commission de l'intelligence artificielle 2024)), or to catch up with the American investment per job level in ICT and R&D assets (€573 billion per year).

However, not only would NGEU need to be renewed for the next five years, but the supplementary private investments to public interventions would also need to materialize. These are not enshrined in financial laws and are not guaranteed.

How can we change the scale of investments in Europe? Given that public funds are limited, it is imperative to accelerate the integration of European capital markets. This is a necessary condition for realizing the private investment leverage that accompanies all public intervention plans. These private investment levers determine the scale and success of industrial policy. They will enable the revitalization of the European productive fabric.

Completing the single capital market requires finalizing the harmonization of clearinghouse rules and, if not merging them, making them interchangeable, allowing the circulation of European savings in common European investments, harmonizing bankruptcy and liquidation rules, and unifying the financial market supervisory bodies.

A change in scale is absolutely necessary as well as a change in the focus. The public spending should be prioritize into specific needs with a clear assessment of the opportunity cost of the chosen priorities. The lack of consensus in the EU is one reason of the dispersion of the financing. In order to satisfy each member's interest EU policies lack the degree of focus needed for efficiency.

We totally agree with the need to create a central European Agency consisting of a panel of scientific and elected politicians which defines scientific priorities and innovative project to invest in (see Fuest et al. 2024)

Section 4. Conclusion: Stick to the European values

This paper shows that digital sovereignty should be a serious concern at the State level not only because it is at the crossroad of geopolitical influence but also because it is an important source of growth.

Is Europe's dynamic legal framework a substitute for the weakness of its market share in the digital economy? It is notable that the EU has been at the forefront in creating regulations governing digital activities, from competition policies to the regulation of private data usage. Equally notable is the fact that Europe hosts fewer dominant companies in the digital economy compared to the United States or China.

The battle is far from lost for Europe, and it has significant legal leverage and considerable human and financial resources to find its place in the global digital economy. However, the fervor of American protectionism on one hand and Chinese technological authoritarianism on the other are undeniably major challenges for the next decade.

As suggested by Bauer & Erixon (2020), digital sovereignty is also a question of keeping the fence around European values. There is undoubtedly a risk of moral superiority but not more than the threat of being overwhelmed by values in contradiction with state of law, freedom of thoughts and democratic principles. At least the design of policies to enhance digital sovereignty should (i) protect the integrity of information which is a pillar of European institutions, (ii) protect the competition and keep fighting against the abuse of dominant position and (iii) feed the scientific and enlightenment legacy of the continent through a massive investment in education.

Diffusion is key to transform a general purpose technology and innovation into productivity and welfare (Unger 2019). The EU concentrates the largest number of persons in absolute and per km with a high level of skills and the largest number of STEMS. Indeed, the United Nations statistics on the number of researchers report 1.42 million researchers in the European Union in 2012, 1.3 million in the US and 1.40 million in China; and per million of inhabitant the ratios rank the EU first with 89,227 researchers while there are 4,018 in the United States and 1,035 in China.

So the EU is then not deprived of rich assets to stay a technological power, but is has to change the scale of its support policy and to seriously handle the dilemma which paralyzed its actions by setting consensual priorities.

References

Affeldt, P. & Kesler, R. (2021), 'Big tech acquisition : Towards empirical evidence', Journal of European Law and Practice **12**, 471–478.

Bauer, M. & Erixon, F. (2020), Europe's quest for technology sovereignty: Opportunities and pitfalls, Ecipe occasional paper, European Center for International Political Economy.

Bellit, S. & Charlet, V. (2023), L'innovation de Rupture: terrain de jeu exclusif des start-ups ?, Les Notes de la Fabrique, Presses des Minies.

Bock, S., Elewa, A., Guillou, S., Nesta, L., Napoletano, M., Salies, E. & Treibich, T. (2024), 'The shortfall in european investment', OFCE Le Blog .

Brynjolfsson, E., Jin, W. & Wang, X. (2023), Information technology, firm size, and industrial concentration, Working Paper 31065, National Bureau of Economic Research.
URL: *http://www.nber.org/papers/w31065*

Commission de l'intelligence artificielle (2024), Ai, notre ambition pour la france, Rapport pour le premier ministre.
URL: *file:///Users/sarah.guillou/Downloads/4d3cc456dd2f5b9d79ee75feea63b47f10d75158.pdf*

Corrado, C., Haskel, J., Jona-Lasinio, C. & Iommi, M. (2016), Intangible investment in the eu and us before and since the great recession and its contribution to productivity growth, EIB Working Papers 2016/08, Luxembourg.
URL: *http://hdl.handle.net/10419/149979*

Ding, X., Fort, T. C., Redding, S. J. & Schott, P. K. (2022), Structural change within versus across firms: Evidence from the united states, Working Paper 30127, National Bureau of Economic Research.
URL: *http://www.nber.org/papers/w30127*

Edler, J., Blind, K., Kroll, H. & Schubert, T. (2023), 'Technology sovereignty as an emerging frame for innovation policy. defining rationales, ends and means', Research Policy **52**(6), 104765.
URL: *https://www.sciencedirect.com/science/article/pii/S0048733323000495*

Europen Court of Auditors (2024), 'Eu artificial intelligence ambition – stronger governance and increased, more focused investment essential going forward', Special Report: (08), 68 pages.
URL: *https://www.eca.europa.eu/en/publications/SR-2024-08*

Fuest, C., Gros, D., Mengel, P.-L., Presidente, G. & Tirole, J. (2024), Eu innovation policy: How to escape the middle technology trap, Technical report, A Report by the European Policy Analysis Group.

Gaglio, C. & Guillou, S. (2018), 'L'europe numérique, entre singularité, faiblesses et promesses', Revue de l'OFCE **158**, 13–36.

Gal, M. S. & Aviv, O. (2020), 'The competitive effects of the gdpr', Journal of Competition Law & Economics **16**(3), 349–391.
URL: *https://doi.org/10.1093/joclec/nhaa012*

Greenwald, B. & Stiglitz, J. E. (2006), 'Helping infant economies grow: Foundations of trade policies for developing countries', AEA Papers and Proceedings **96**(2), 141–146.

Griliches, Z. (1998), R&D and Productivity: The Econometric Evidence, University of Chicago Press.

Guillou, S. (2023), La souveraineté économique à l'épreuve de la mondialisation, Ed. Dunod.

Guillou, S., Bock, S., Elewa, A., Nesta, L., Napoletano, M., Salies, E. & Treibich, T. (2024), 'Documenting the widening transatlantic gap', OFCE Policy Brief (129).

Guillou, S., G'Sell, F. & Lechevalier, F. (2024), 'Buy european tech act', (1).

Haskel, J. & Westlake, T. (2017), Capitalism without capital, Harvard University Press.

Janßen, R., Kesler, R., Kummer, M. E. & Waldfogel, J. (2022), Gdpr and the lost generation of innovative apps, Working Paper 30028, National Bureau of Economic Research.
URL: *http://www.nber.org/papers/w30028*

Khan, L. M. (2017), 'Amazon's antitrust paradox', The Yale Law Review (126), 710–802.

Mafhouz, S. & Pisani-Ferry, J. (2023), Les incidences économiques de l'action pour le climate, Rapport à la Première Ministre.

Nicoletti, G., Vitale, C. & Abate, C. (2023), 'Competition, regulation and growth in a digitized world', (1752).
URL: *https://www.oecd-ilibrary.org/content/paper/1b143a37-en*

Noy, S. & Zhang, W. (2023), 'Experimental evidence on the productivity effects of generative artificial intelligence', Science **381**(6654), 187–192.
URL: *https://www.science.org/doi/abs/10.1126/science.adh2586*

Shelley-Egan, C. & Vermaas, P. (2024), 'European technological protectionism and the risk of moral isolationism: The case of quantum technology development', Journal of Responsible Technology p. 100084.
URL: *https://www.sciencedirect.com/science/article/pii/S2666659624000106*

UNCTAD (2021), Digital economy report 2021, Technical Report Cross-Border Data Flows and developement, UN, Geneva.

UNCTAD (2023), Technology and innovation report, Technical report, United Nations.

Unger, R. M. (2019), The knowledge economy, Verso.