ePaper | March 2024

IS THERE A EUROPEAN WAY TO CLOUD COMPUTING?

THE MATRIX

LESSONS FROM AN UNFULFILLED ENDEAVOUR IN THE GOVERNANCE OF DIGITAL TRANSFORMATION

EDITED BY
MARCO BERLINGUER

transform! europe

www.transform-network.net

TABLE OF CONTENTS

IMPRINT

2024

transform! european network for alternative thinking and political dialogue
Square de Meeûs 25 - 1000 Brussels, Belgium

transform! europe is partially financed through a subsidy from the European Parliament.

Layout: Vittorio Giannitelli
Cover design: Vittorio Giannitelli

EXECUTIVE SUMMARY

The European Union has set itself the goal of achieving its own "digital sovereignty". This is but one of several reasons why it is particularly interesting to study the ongoing attempt by European governments and the EU to regain an active role in the digital revolution, to develop a new type of industrial policy, and to intervene through political decisions on technological development itself. And these reasons also have to do with the context in which the European initiative is taking shape.

Indeed, a number of new infrastructure technologies are currently being designed and rolled out. Cloud computing, the Internet of Things, 5G, and Artificial Intelligence constitute the core of these new technological systems. Collectively, they represent the advent of a new stage of the digital revolution, which is destined to have a radical impact on all activities, economic sectors, organisations and political institutions themselves.

Added to this is a clear return of public intervention in the governance of technological and economic development. This is the result of the importance of these new infrastructure technologies, the explosion of geopolitical competition between the US and China over the control of these new technological frontiers, and the crisis of neoliberal globalisation.

There is one last reason why this subject deserves particular attention. In this new phase of the digital revolution, new forms of governance will be tested and established to address the multiple challenges of this same technological, economic and political transition.

*****

To understand the nature of this transition and the characteristics and limitations of the European initiative, this essay analyses European policies in the field of cloud computing. Cloud computing is the most mature of these technologies and its deployment is already on the agenda of all major governments. It is also a paradigmatic infrastructure, in the sense that it incorporates multiple characteristics exemplary of this phase of transition in digital transformation and of the main technologies that are promoting it. It represents the shift to an infrastructure-like use and consumption of digital and computational technologies. It is an enabling infrastructure for the transition to a society based on the intensive exploitation of data and computational capabilities. It is an infrastructure whose introduction destabilises and reconfigures the modes of operation and even the boundaries of economic sectors, organisations, and institutions. Finally, it is an infrastructure that is extremely complex, in its components and architecture, and subject to constant dynamism. All these characteristics make it emblematic and, likewise, impart a push toward the introduction of new forms of governance.

*****

The EU identified the importance of this shift to cloud computing back in 2012. And in the 2019-24 parliament, regulatory activity and promotion of initiatives has intensified. However, the EU has so far failed to reverse the trend toward a deepening of the structural dependence of the European economy and public administrations on a few oligopolies, mainly from the United States, who dominate the cloud-computing market.

Still, there have been so many actions in recent years that it has become difficult to maintain a coherent and up-to-date picture of the totality of these initiatives, which often overlap, intervening into the same issues. The second part of this essay is devoted to putting all this material in order.

There are in fact four strategic statements, fifteen pieces of legislation and at least eight initiatives that directly or indirectly relate to cloud computing.

*****

The overall goal of all this activity can be encapsulated in the notion of digital sovereignty. On closer inspection, however, the notion of sovereignty has taken on at least two distinct meanings. The first, which is more classical (although it is asserted by a Union of states) corresponds to the determination to regulate the digital sphere. The EU in this sense is — along with China — the political system that is pioneering new legislation in many areas of digital development.

In contrast, the second meaning is more innovative, and refers to the goal of preserving — for individuals, organisations, and governments — conditions of autonomy, self-determination, and freedom of action and choice within the new digital environments.

Concretely, the initiatives undertaken by the EU and individual European governments operate along three complementary lines of action.

*****

The first is the regulation of the new digital platforms and critical infrastructures. It thus de facto recognises the nature of many digital technologies as *essential services*. Regulations encompass multiple subjects, given the critical and pervasive nature of these infrastructures. They range from the protection of users' fundamental rights and the freeing of users and businesses from unsupervised private rules, to the introduction of transparency on algorithmic content moderation and prioritisation, and the introduction of rules to ensure "sovereignty" over data, or immunity from surveillance by non-European authorities. On the economic side, the main concern is to protect users and businesses from power asymmetries vis-à-vis platforms and "gatekeepers", and the possibility of these latter committing abuses due to their dominant position. The most ambitious goal is to increase competition by beginning to break up monopolistic positions, for example by mandating the interoperability of services on these platforms.

*****

The second line of action is industrial policy. Edge computing and industrial data have been identified as the two main opportunities for European industry. Edge computing is considered the next evolutionary stage of cloud computing and is expected to accompany the exponential increase in data flows made possible by the Internet of Things and 5G. In addition to being a new technological frontier, edge computing requires a more decentralised architecture for data and computational resources and open communication protocols. Thus, it can help advance the goal of disrupting the centralised, closed and proprietary systems that currently monopolise cloud-computing service offerings. The intensive use of data in industrial processes is a new frontier, on which the EU aspires to build a leading ecosystem of innovation based on its strength in traditional manufacturing, which potentially provides a rich source of strategic data for the development of innovative services.

In both areas, the EU aims at leveraging the size of its market and its regulatory leadership to become a "trustworthy" global standard-setter.

*****

The third line of action is the preservation of security and sovereignty over citizens', businesses' and governments' most sensitive data. In the wake of the pioneering GDPR, an important part of EU initiatives and legislation has been dedicated to this goal, as in the cases of Gaia-X, the EUCS under discussion within ENISA, the European cybersecurity agency, the new rules on the regulation of critical infrastructure, and the new legislations on data governance. The EU aspires to make these superior legal data-security guarantees its own competitive advantage - and a tool to overcome the main barrier to cloud adoption and data exploitation, namely the prevalent lack of trust among companies, citizens and institutions. Second, these security requirements can form the basis for making critical infrastructure into a protected market in which to grow an autonomous European industry and set of systems and technology standards.

*****

So, will the EU achieve digital sovereignty?

In the abstract, it is possible to glimpse the outlines of a technological, regulatory and industrial strategy that advances toward the goal of achieving greater European digital autonomy in cloud computing. The outlines of this strategy are succinctly spelled out in the Berlin Declaration of the 2020 European Council. The principles on which that document relies for building sovereign cloud infrastructures in European public administrations are: interoperability, open source, standardisation, and modularity.

The EU has also freed up significant resources with the Next Generation EU fund, 20 percent of which - about 160 billion euros - is prescribed to be dedicated to investments in the digital sphere. Despite this, the implementation of this strategy has been uncertain and inconsistent.

The most critical step is the migration to cloud computing of European administrations, due to the scale of investments required and the need to preserve the security of the most critical data, which has led major European countries to exclude non-European or non-domestic providers from their management. This essay analyses the plans presented by Italy, France and Germany - the three largest European economies - for migrating their administrations to the cloud.

The main weaknesses that emerge are: a lack of clarity on common objectives, the absence of coordination among European governments, and the lack of an effective digital policy governance system. But a further difficulty is posed by the highly innovative nature of the industrial policy that the European strategy seems to require, due in part to the absence of an autonomous European digital industry.

*****

Overall, then, the new European digital policies must be seen as an unfinished attempt.

What can we learn from this attempt?

In the third part of this essay, we answer this question, following what is perhaps the most original insight followed by the European strategy: the specification of a set of design and technology development principles as a guide for building sovereign cloud-computing systems.

Those principles - interoperability, open source, standardisation, modularity - are, on closer inspection, ones widely used in the construction of software systems.

In this essay we propose to consider them as components of a matrix that has come progressively to the fore with the development of information and communication technologies and software in particular.

*****

What is behind this matrix's success?

The main explanation is that these principles constitute a set of strategies that respond to the need to manage the increasing complexity, scale and integration of software systems, and their constant dynamism. In turn, the adoption and use of these principles has further facilitated the growth in the complexity and dynamism of these systems.

Moreover, this matrix belongs to a new family of organisational forms that have become increasingly important along with the development of the digital revolution and which are notably different from the ones typical of the Fordist era.

*****

The main and most innovative of these principles is Free and Open-Source Software (FOSS). It is, in fact, a digital commons: its proprietary form allows anyone to use, study, modify and redistribute the software. Despite this, it has taken a foreground role in the production of software, i.e., the leading technology of the digital revolution.

Moreover, its non-proprietary logic has expanded and exerts a growing influence on the other principles and their governance models. This means that already today - and predictably even more so in the future - the core of digital infrastructure is developed and regulated by nonmarket forms of governance, which are based on novel forms of collaboration and competition.

Moreover, one of the features of this matrix is that it shapes but also eliminates markets and liberates productivity according to a different logic. These characteristics are among the most underestimated aspects of the EU approach.

*****

But what does it mean to find these principles of technological design and development stated as tools in a political document?

Primarily, it means two things. The first is that this matrix offers new levers to govern digital ecosystems. This is something with which Big Tech companies are already familiar. What is new is that policy is now beginning to test its use in regulating new digital infrastructure and implementing a new kind of industrial policy. We are still in the early stages and in an experimental stage, but we can expect a gradual acquisition of clarity, capacity and, in the future, more decisive actions based on these new tools.

*****

The second, related implication is that we are entering an important new phase of evolution in the forms of governance of this matrix. If we look at the trajectory of FOSS, two phases can be distinguished: the first hegemonised by developer communities, the second by enterprise adoption and new forms of market competition. As a result of this trajectory, a series of hybrid organisations and arrangements have emerged. The most obvious example are the large foundations that have sprung up within the FOSS ecosystem. Governments' organic entry into this ecosystem heralds the advent of a new stage in this evolution.

This is not a phenomenon limited to the European case. Rather, it depends on the systemic and infrastructural role that FOSS has come to play, the scope of latest digital technologies that are being designed and implemented, and the intensification of international competition.

*****

This means that in the near future we will see the emergence of new forms of governance, which we can call second-generation hybrids, which are likely to play a much larger and even systemic role.

Although indicators pointing in this direction are present in all initiatives promoted by the EU and major European governments, a clear awareness and explicit thematisation of this kind of challenge is still lacking in European strategy.

INTRODUCTION: WHAT GOVERNANCE FOR DIGITAL TRANSFORMATION?

The countries of the European Union have so far failed to play a leading role in the digital revolution. Instead, they have accumulated technological and economic dependencies which - in the face of the accelerated transformations produced by the latest generation of digital technologies and the concentration of power and wealth they are producing - risk compromising both their autonomy and future prosperity. This risk has led the European Union, in the current legislature, to invest in a series of initiatives – legislative or otherwise – to improve EU's digital autonomy.

This rethinking moreover takes place in a world in which the Washington Consensus is fading, free-trade principles and global supply chains are being destabilised, and industrial policy, security imperatives and protectionism are making a strong comeback, especially on the most advanced frontiers of technological innovation (Sullivan, 2023a). Overall, for the EU this means abandoning its *laissez faire* policy and undertaking a radical reorganisation of its policies. Thus, digital policy, in this context, is going to be one critical testing ground for the EU's revived industrial and technological policy ambitions (Prisecaru, 2019; Mazzucato & al., 2021; Terzi & al., 2022).

If we had to choose one term to summarise all the digital policy initiatives undertaken in this legislature by the European Union, the main watchword would be "digital sovereignty". This is a concept and a goal that has been stated in a series of documents and declarations of the European Parliament, the European Commission and the European Council. However, quite frankly, if we were to ask ourselves: in light of all the initiatives undertaken, will the EU be able to achieve its strategic autonomy in the digital sphere, the short answer would most likely be: "no". There are far too many reasons for scepticism. The list is a long one: the build-up of delays, previous failures, the absence of a robust digital ecosystem, an inadequate governance system, political divisions, a divergence of interests, and a lack of geopolitical autonomy.

Yet, it is still worth trying to give a longer answer. Because the EU is engaged in a challenge of great significance. In fact, the entry of a constellation of new general-purpose or infrastructural technologies - such as Cloud computing, the Internet of Things, 5G, AI - will deepen and accelerate the digital transformation in the forms of production, in administrative systems, and in practically every social activity. And the next generation of digital technology systems that are currently being designed, developed and implemented will require major innovations in governance systems, if only because of their scope, scale, complexity and dynamism (Northrop & al., 2006). Added to this, a new political climate is forming, marked by the return of the political will to govern technological development. In summary, **we are entering a new phase of the digital revolution** (Castells, 2004; Perez, 2010), and in this new phase it is very probable that **new typologies of governance systems are going to be tested and take shape**.

It is from this perspective, therefore, that it is most interesting to investigate the constellation of initiatives that are marking the shift in EU digital policy. That is, we ought to see it as a tentative and uncompleted attempt to address **a new typology of challenges** for governance systems. Indeed, the insufficient clarity about the nature of the challenge ahead should be added to the long list of obstacles that make it difficult to imagine European ambitions being crowned with success.

The main objective of this essay is to delve into this direction and help to better understand some aspects of this challenge that is marking the advance of the digital revolution. To this end, we are going to focus on one of these technological systems: cloud computing. This is the most mature of the new technological infrastructures today in the process of being rolled out. In 2020, the EU presented a series of strategic statements on digital policy and cloud computing, aimed at improving its digital autonomy (see Figure 6). Since then, it embarked on a new path which has been supported by initiatives, funds and legislation. In this area, as in others, the first lever that the EU has identified to regain autonomy is the regulatory instrument. The EU has 450 million citizens and is one of the world's largest markets. According to some estimates, the EU market accounts for 75 percent of the external markets for large US technology companies, for example (Barker, 2020). This gives it a powerful lever and, as we will see, the EU is using it in an increasingly determined way. So much so, that it has become difficult to maintain a coherent and up-to-date picture of all the legislative initiatives that are piling up. But even so, the regulatory instrument is hardly enough. Moving forward, the EU is beginning to abandon its self-imposed cage and leave behind *laissez faire* and the market as the alibis behind which it has long managed to avoid making tough policy decisions and innovations in its system of governance.

Of course, what adds further complexity to the EU initiative is that it takes place in the political context of a union of states, each jealously maintaining its own sovereignty. As if that was not enough, digital policy is one of the most decentralised areas of policy, also internally in each of the nation-states. For the EU this is a major challenge, which makes it extremely difficult to design and maintain ambitious and coherent European policies.

How will the EU cope with this? This is hardly clear at this point. And, as we said, maintaining a sceptical attitude is more than reasonable. However, two points appear clear enough at first glance. Realistically, EU digital policy lacks several elements to make it an organic and successful strategy. At the same time, it is undeniable that the EU has developed an ambitious and innovative agenda in recent years. Overall, the EU policy on cloud computing can be seen, precisely, as an unfinished attempt to develop an innovative industrial policy model for the large and complex technological systems that characterise today's digital technologies. And it is from this perspective that we will examine the EU strategy for cloud computing, in the concluding third part of this essay. The goal will be to identify some distinctive characteristics that are likely to inform new types of governance systems in the next phase of digital transformation.

The first two parts of this essay will be dedicated to an effort of clarification and systematisation. In the first part, we will make a brief introduction to cloud computing. We will describe what it represents as a new infrastructure and as a new approach to the production of and access to digital services. We will outline the main barriers to its adoption and the main risks in terms of dependency, security and lock-in that cloud computing poses for all types of organisations. We will hint at its potential transformative impact on organisations and institutions, included public administration, which represents a further source of challenges and concerns. What is more, cloud computing has an "enabling" function for the ongoing data-driven shift in the economy and society, which further explains its strategic importance. Finally, we will briefly describe the complexity and dynamism that characterise cloud computing technologies - as in general the current generation of digital systems - which constitute a further challenge for the resurgent ambitions of industrial and technological policy intervention.

In the second part, on the other hand, we will reconstruct the motivations behind the evolution of EU digital policy. We will clarify the double meaning that "digital sovereignty" has taken on in EU documents: as a desire to ensure compliance with the rules set by the EU itself and as an aspiration to preserve the freedom of EU citizens, governments and businesses to act and decide in the new digital environments. We will outline the main political and economic concerns that have gradually led the EU to change its approach and progressively abandon the laissez faire philosophy in digital policy. We will then reconstruct in schematic form the abundant legislative output and the other initiatives promoted by the EU around cloud computing.

We will summarise and schematise the main features of the European cloud-computing strategy as it has taken shape during the current European legislature and we will unpack the long-term competitive vision which is guiding the initiatives: i.e. that of fostering a strategic positioning of European industry in the next generation of cloud-computing architectures and in the future economy based on the exploitation of industrial data. To conclude this part, we will also mention the limitations that the first implementations of this strategy are encountering, looking at European public administrations' migration to the cloud as the most critical step underway. Indeed, given their scope and criticality, digital public-administration systems represent the cradle or the grave of European aspirations to digital autonomy. In theory, we shall see, it should be possible to glimpse the outlines of a strategy for this migration, which is at the same time a technological, regulatory and industrial process. Yet, in reality, political hesitations and unresolved structural weaknesses make the situation hardly encouraging for EU ambitions.

Finally, in the third part we will delve into what is perhaps the most original feature of the EU's strategy. It is one particular aspect of the EU's digital strategy on cloud computing. This is a group of principles of architectural design and technological development that the EU has identified as guiding, at least in principle, its digital policy on cloud computing. The principles, to which the EU has entrusted a significant part of its chances of regaining digital strategic autonomy, are: **open source software**, **standardisation**, **modularity**, **and interoperability**. In this final section we will frame these principles as a matrix – and we will use this latter as a peculiar lens through which to investigate still insufficiently addressed innovations in governance systems. To this end, we will explore the forces that have brought this matrix of principles to the forefront in digital technology, and not simply in EU policy.

In doing so, we will give a special importance to FOSS as an innovative arrangement and institutional approach to software production.

Free Software AND Open Source Software

BOX 1

Free and Open-Source Software is a protagonist in the software scene and in cloud computing. It made a long journey to reach this position. We will return to some aspects of this journey in the third part of this essay. For now, we shall offer a clarification on the expression Free and Open-Source Software.

As a rule, this essay uses the broader, unified definition of Free and Open-Source Software and the acronym FOSS. Sometimes, however, the definition "Open-Source Software" and the corresponding acronym OSS are instead used; they are today more common, including in EU documents. The different definitions originate from a split that occurred in the late 1990s, promoted by a component of the Free Software movement. The definition of Open Source had the goal of "depoliticising" the movement's image, with the aim of presenting the features of Free Software in a more business-friendly way. At the substantive level, the main difference is that the Free Software movement remains more tied to the use of the so-called "copyleft" clause introduced by the General Public License, created by Richard Stallman, which requires maintaining the same type of license even in derivative versions of software that integrate, extend or modify software released under this type of license.

Meanwhile, Open-Source component is friendlier with the use of so-called "permissive" licenses, which do not hinder any kind of use and evolution of the software, even if it is proprietary. Of course, in the latter case the software ceases to be defined and recognised as open-source, as it loses the essential characteristics, which also for open source remain the 4 freedoms originally defined by Richard Stallman. On this fundamental definition, there is no difference. Free and Open-Source software, to be worthy of the name, must guarantee the four basic freedoms to use, study, modify, and redistribute the software.

These four characteristics constitute the universally recognised criteria within FOSS for recognising a license as belonging to this definition The two main organisations that oversee the compliance of different types of licenses with this definition are the Free Software Foundation (FSF) and the Open Source Initiative (OSI). Although today the coexistence between these two components of the FOSS movement has lost its polemical connotations, it cannot be ruled out that the continued spread of the social use of FOSS and the return of a "political" approach to FOSS, albeit with different connotations from those of the movement at its origins, may bring back to the forefront the importance of the copyleft clause, for the purposes of a more effective and equitable management of the benefits and burdens of FOSS and a better handling of the contradictions generated by its success.

(For more on this, see the third part of this essay)

The centrality given to FOSS is justified for two reasons: its outstanding success in the core technology of the digital revolution and its growing influence on the evolution of the other principles of the matrix. While we will refrain from proposing a one-size-fits-all or techno-determinist explanation, we will nonetheless focus on the increasing complexity of digital systems as the main force that has propelled this constellation of principles – and their growing entanglement – to the forefront of digital technology design and development. And further delving onto the characteristics of this matrix, we will identify some evolutionary trends and some emerging areas of innovation in the governance of present (and predictably future) large and complex digital systems.

These innovations will revolve – according to our argument - around **1) a bolder use of this matrix** as a tool to manage the complexity and dynamism of these systems, but also as a lever for the political and economic governance of digital ecosystems; **2) the recognition of the role of collaborative dynamics as a central driver of wealth generation** and of this matrix as a tool for both creating and eliminating markets; and finally **3) the emergence of tripartite systems of governance**, which will have to recombine the logic of markets, commons and public powers in innovative ways, in a context of technological development which is going to be much more politicised.

Though, at an embryonic level, these innovations can be seen sprouting behind many EU policy initiatives in the field of cloud computing, they still await to be fully addressed in the EU vision and strategy. It is, in any case, around these areas - this will be our concluding thesis - that we are likely to see a new kind of public intervention and public policy take shape, and, broadening the perspective further, tackling these issues will constitute a critical component of a new kind of mixed economy and a terrain of competition between alternative systems in future digital transformation.

1

CLOUD COMPUTING:

AN INFRASTRUCTURE FOR A DATA-DRIVEN SOCIETY

1.0

CLOUD COMPUTING AS A UTILITY

But we should start with the basics. What does migration to cloud computing mean and imply?

In general, cloud computing refers to the provision of computing resources, such as servers, storage, and applications, via the Internet, rather than on-premises (European Commission, 2012).

On an economic and organisational level, it is a shift to an **infrastructural use** of computing resources of all kinds from networks to servers, from hardware to software applications, along the lines of other **utilities**. It can be conceived as a transformation similar to that experienced by factories in the 20th century, when they stopped producing their energy locally, with furnaces for example, and instead connected to the electric grid. In this case, local servers are replaced by an enormously scaled and indeed much more centralised system (Gong & al., 2010).

This is the "public cloud" model, i.e. a cloud that is shared by a generic audience and many users. But there are also private cloud models, where servers, services and data are shared only within a delimited organisational boundary; and also hybrid systems where the public and private models are variously combined (Huth & Cebula, 2011).

In any case, the fundamental economic and organisational principle of the cloud is based on the sharing of resources and on their standardisation. Individual organisations are freed from the need to invest in local infrastructural resources and from having the internal burden and expertise required to manage them. It is basically a process of externalisation and outsourcing. On the other side, cloud service providers (CSP) exploit economies of scale and make more efficient, flexible and rational use of resources.

Technically, the key innovation has been **virtualisation**: the virtual and simplified replication of hardware and software resources, allowing for more flexible and largely automated management and deployment of these resources, often through user-friendly interfaces (Malhotra & al., 2014; Jain & Choudhary, 2016). For example, simplified and specialised versions of operating systems or dedicated channels for data transmission. The creation of virtual versions of hardware and software resources means that these can be quickly and flexibly generated, made available and allocated according to variable customer requirements. They are paid for according to usage ("pay-as-you-go"). For instance, it makes it possible to respond quickly and flexibly to peaks in demand, without having to make infrastructure investments that would be uneconomical once those peaks have passed, i.e. because they would produce excess resources that would be useless.

The "platform shift" to cloud computing has also impacted the way in which services are created, delivered and accessed. The shift of hardware infrastructure to the cloud is also functional to a reorganisation of the access and provision of software services and data storage and processing.

Conventionally and in the prevailing commercial offer, these services are often organised on three levels of the technology stack.

- Infrastructure as a Service (IaaS): which refers to resources such as processors, storage units, and networking bandwidth;
- Platform as a Service (PaaS): which refers to resources such as databases, application development frameworks, big data analytics engine, and AI/ML frameworks;
- Software as a Service (SaaS): which refers to resources such as user-facing applications of the type of email, messaging, video-conferencing, and document-sharing.

Cloud solutions are usually "sold" on the market with the promise of lower costs. However, this is not always true. It depends on the type of use made of these resources. The main advantages are flexibility and outsourcing. These advantages can be exploited by organisations that prevalently use communication and computing services, but also by companies producing software services, start-ups or application vendors who can concentrate on their core business and benefit from a very flexible and standardised infrastructure.

The problem of the real costs of migrating to cloud computing must be contrasted with the main risks associated with this model. The main risk of cloud computing comes from **dependence** on vendors for essential services and for managing the most sensitive data. And one of the main reasons for concern and resistance to migrating to the cloud is the fear of lock-in, i.e. of being "trapped" by a vendor (Opara-Martins & al., 2016).

Indeed, there are multiple **lock-in** mechanisms, across know-how and technology formats, that can make it extremely difficult and costly to switch vendors and technology once one's systems are migrated onto a vendor's infrastructure. Moreover, these mechanisms - in the absence of common standards and interoperability rules - are deliberately created through technology and business strategies by vendors. For instance, large vendors typically offer - especially to large customers and governments - very advantageous and, even below- cost entry conditions for their services, particularly infrastructure services, in order to secure long-term future returns in higher value-added services in this way. This risk of lock-in must also be considered in light of the clear and strong trend toward concentration of this market in the hands of a few providers.

1.1

THE TRANSFORMATIVE IMPACT OF CLOUD COMPUTING

On the other side, as for other utilities, cloud technology can be regarded as a democratisation of the access to the most advanced information technologies. After all, it provides homogeneous access to high quality services – regardless of the size of the organisation, its resources or its geographical location – including advanced technologies such as AI. (Chinese cloud providers even recently launched two cloud platforms designed to allow the general public to make use of experimental quantum-computing machines).

However, the impact of cloud computing, in the longer perspective, is wider and deeper. The migration to cloud computing is in fact often associated with the concepts of digitisation, digitalisation and digital transformation. Though these concepts can be used with various meanings, digitisation is mainly used to refer to the trend towards the digital reproduction of everything: that is, the reproduction of processes, resources, organisations in digital formats and modes. Digitalisation and digital transformation are instead used to refer to the transition to an 'industrial' phase of the digital revolution - the industrial internet, as it is sometimes called - with the massive application of economies of scale, automation and standardisation to computational resources and data. But it is also used to refer to the radical and structural changes that the penetration of the latest generation of digital technologies (Cloud, 5G, IoT, AI) is expected to have on the organisation of every business, sector, activity and institution (Brennen & Kreiss, 2016; Bloomberg, 2018; Vrana & Singh, 2021).

But the point here is that, along with the deployment of cloud computing and the new generation of digital technologies, deep and radical reorganisations are expected to progressively impact economic activities, value chain structures, and sector delimitation. This promise or threat of radical organisational and institutional transformations surely a further explanation - beyond the concern for one's own sensitive data and the fear of lock-in - as to why in reality, in spite of political agendas and business strategies pushing for a rapid adoption of the cloud, there are multiple barriers, difficulties and resistance that often make consultancies' forecasts of a rapid and exponential growth of the cloud market implausible.[i]

A good example to understand the barriers that may be encountered along this transformation is **public administration** (Barcevičius & al., 2019). It is difficult to speculate on what the long-term effects of a migration to cloud computing will be in terms of the reorganization of the public administration. One can imagine that even the relationship between public administration and society will change for there will be greater integration and sharing of data, services and systems between the public, the private and the social sectors.

A good example for understanding the barriers that may be encountered along this transformation is **public administration** (Barcevičius & al., 2019). It is difficult to speculate on what the long-term effects of a migration to cloud computing will be in terms of the reorganisation of the public administrations. One can imagine that even the relationship between public administration and society will change, for there will be greater integration and sharing of data, services and systems between the public, the private, and the social sectors.

But just limiting ourselves to public administrations, cloud computing is bound to structurally impact the way in which public services will be designed and delivered and will structurally change the internal organisation of public administrations and their horizontal and vertical relationships. Because it will inevitably impact on the distribution of functions and competences at the different territorial (sub-national, national and supra-national) levels and in the different sectors – foreseeably with mergers, reorganisations and restructurings that are still difficult to predict at the moment, but which will surely be profound. This is especially true since the management of ICT services in general has so far been extremely decentralised and the push will in most cases be towards centralisation and standardisation, with common infrastructures, platforms, data centres, and services which will be shared across territorial and sectoral levels.

All these potential transformations also explain why, coinciding with the migration to the cloud, a global debate on "digital **sovereignty**" has opened up. In Europe, the debate involves many dimensions; we will return to it later. One involves the concern about the potential outsourcing of critical and essential data and services to extra-EU private entities, subject to extra-EU political authorities. But it also reflects the internal drive towards the creation of a single European internal market and greater homogeneity and centralisation of decisions, norms and standards at the European level, which is not going to be an easy undertaking.

1.2

CLOUD AS AN ENABLING INFRASTRUCTURE

Like most digital markets, the cloud-services market is extremely concentrated. Thanks to cheaper, more integrated, efficient and functional commercial offers, the market is dominated by a very few oligopolies. This means three, above all: Amazon, Microsoft and Google.

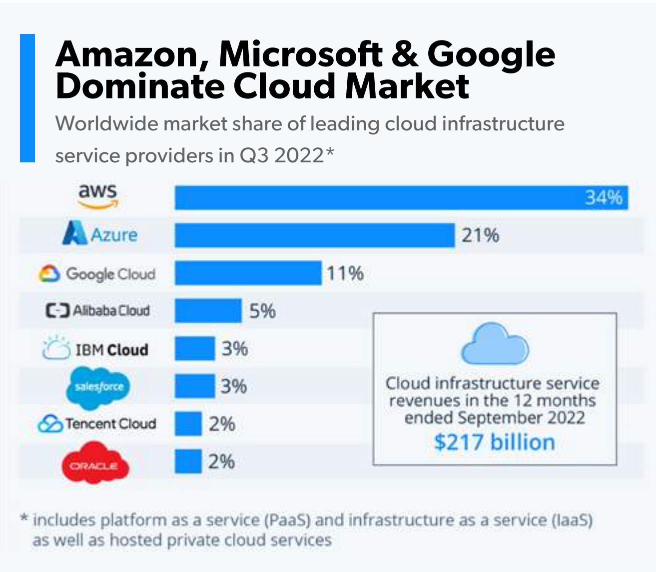


Figure 1 — source: Synergy Research Group

The only other provider with significant global market shares is Alibaba (see Figure 1). Moreover, as is the case in most digital markets, once a dominant position has been created, it is self-reinforcing – and it will be extremely difficult to open up space for alternative competitive offers. For example, the collective market share of the European players in the European cloud infrastructure services sector has in the last five years shrunk from 27% to a mere 13%.

Thus, in absence of strong corrective interventions, cloud computing migration risks reinforcing the wider monopolistic structure of the digital economy. This is not least true because the cloud is actually an **enabling** and preparatory technology for the deployment of a set of new emerging technologies, beginning with IoT and AI.

Indeed, one of the most important stakes in play behind cloud computing concerns **data**. Cloud computing is an enabling infrastructure for data collection and data processing. And it is precisely from the massive use of this data combined with the use of Artificial Intelligence (AI) - whose progress in turn feeds on these same processes of data storage and exploitation - that a new frontier of **innovation** and knowledge is expected to open up, and likewise a profound reorganisation of production chains, and the creation of a new world of services, products and markets.

Indeed, the crucial importance of data has led to talk of "data capital", to describe the most innovative forms of capitalism, driven by a logic of "data accumulation" (Fourcade & Healy, 2017; Sadowski, 2019). More generically Chinese doctrine defines data as a "new productive factor" or a "new productive force" (Pao, 2021). While EU documents instead use the expression of a "data-driven society" (Barcevičius & al., 2021).

This role in digital transformation and "datafication"(Mayer-Schönberger & Cukier, 2013) - the transformation of information into formats that can be used and processed by algorithms and digital systems - is in any case what strategically makes the cloud so important, and at the same time critical.

It explains the will of governments - for instance of the European Union and China - to accelerate the adoption of the cloud in order to move early on this frontier of innovation, to avoid falling behind the USA even in this critical step of the informational revolution. It also explains the great risks involved in this race. This means risking a loss of control over one's most critical data (its "expropriation"), capture and dependence on opaque technological systems over which one has no control, but also risks of vulnerability that may arise from the trend towards centralisation and homogenisation of cloud systems.

1.3

A NEW KIND OF INFRASTRUCTURE

We can thus think of cloud computing as a critical infrastructure, which will develop in integration with other emerging technologies, such as Artificial Intelligence, the Internet of Things and 5G.

But one clarification needs making. The digital era relies on different kinds of infrastructures from those of the industrial era. And to the extent that the concept of infrastructure refers to a stable foundation, it can be misleading. In fact, cloud computing, like information or digital infrastructures in general, has a **complexity** and **dynamism** both in its components and in its architecture that do not conform to this characteristic associated with the idea of infrastructure. This is a highly relevant aspect at a time when policy, public intervention, are preparing to resume a role in directing the development and technological innovation and governance of these infrastructures.

It has been said that "the current state of our digital infrastructure is one of the most poorly understood problems of our time" (Eghbal, 2016). If we limit ourselves to software, which constitutes the central component of digital technology and of the new infrastructures (along with data and "datafication")[ii], the picture is indeed overwhelming complex.

If one analyses software systems, most software today is built on the basis of hundreds if not thousands of direct or indirect "**dependencies**".

That is, software systems are created by assembling dozens or hundreds of existing software components, or libraries, or modules (first-level dependencies), which are then in turn composed of components (second-level dependencies). And so on. This happens in the vast majority of cases without either the provider or user of the resulting services having any real awareness of the origin or current status of the management of all these components.

However, each of these components requires continuous maintenance, either to fix and solve problems that arise in its operation, or to integrate new features and functions, or to remain up-to-date in relation to the evolution of the other systems with which it must integrate and communicate (Fadhlurrahman, 2023).

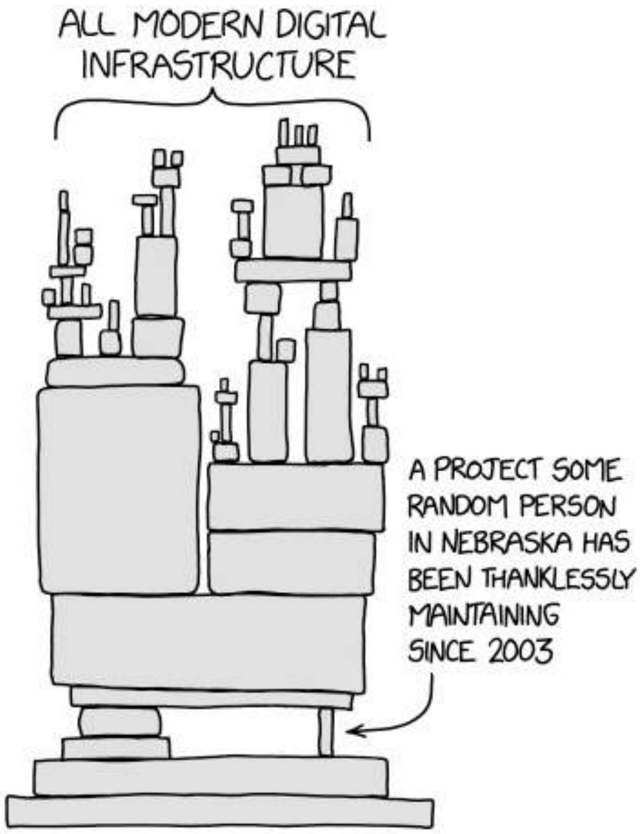


Figure 2 — XKCD: Dependency by Randall Munroe (CC BY-NC 2.5)

The result is an increasingly intricate and interdependent complex of multi-layered strata that compose existing digital systems and infrastructures that opens up great challenges in terms of both understanding and governance (Bratton, 2015).

Moreover, an estimated 70 to 90 per cent of all these components of currently existing software systems are open-source (Synopsis, 2023). Indeed, the success of OSS is due in large measure precisely to the increasing complexity of these systems and the ease of use, assembly, adjustment and recombination that open-source software allows (Berlinguer, 2021). This feature, however - and we will come back to this point - in turn further increases the complexity of these infrastructures and of their governance (see Figure 2).

Sticking with the infrastructure metaphor, it is another characteristic conventionally associated with infrastructures that they tend to go unnoticed, until some problem arises or they cease to function (Edwards, 2003). This is also what has happened – and is happening – with digital infrastructures. Episodes of unexpected vulnerabilities that suddenly affected millions of organisations have often allowed these latter, and indeed governments, to see a jungle of "dependencies" which they had hitherto completely ignored.

Ultimately, these infrastructures bear great internal complexity. Somewhat like living organisms, they are constantly changing and require constant care, maintenance, development and updating (Arthur, 2009).

Secondly, the very architectures of these infrastructures are subject to restructuring, which in certain cases may even be radical. The architecture of the cloud itself provides such an example. During its first decade of existence, cloud computing has been settling - also due to the boost given to its evolution by the large US hyperscalers - into a strong centralisation, not only in the commercial offer, but also in its technological architecture. The main cloud-computing services currently on the market are offered as highly centralszed models in large data centres. And they are provided as integrated, private and closed systems, despite the fact that an important part of their components is open-source.

However, despite this trajectory and this set-up, the predominant expectation at the moment is that cloud computing is moving towards a different, more decentralised and federated evolution, and that these hyper-centralised architectures represent a barrier that will need to be deconstructed. The term for this evolution is Edge-Cloud or **Cloud-Edge-IoT** (Villari & al. 2016). In the EU, the definition of **Continuum Computing** has more recently emerged . Even leaving aside the many political and economic factors pushing in the same direction, there are also technical reasons for this. In fact, this evolution is mainly required for the adaptation of the cloud paradigm to the Internet of Things (IoT) phenomenon, which is going to deploy billions of sensors collecting and processing information in every sphere of social life. The Edge Computing model aims to provide processing and storage capabilities as an extension of IoT devices, without the need to move data and processing to a central data centre. This reduces communication delays, costs and the overall size of the data that must be moved over the Internet. This need will find many applications in future functionalities, such as in Industry 4.0 or driverless mobility. In any case, this new architecture requires an **orchestration** between cloud resources and resources at the edge of the network, according to a distributed, federated model, which will require protocols, standards and **interoperability** between systems, which is not possible today, due to the predominantly closed, proprietary and centralised nature of cloud systems. Similar disruption is expected from the large-scale integration of AI into the cloud infrastructure, although it is still too early to venture such scenarios.

Ultimately, however, the fact remains that potential radical transformations form a backdrop that makes the task of recovering political governance over these technological systems complex.

We will return to this challenge in the third part.

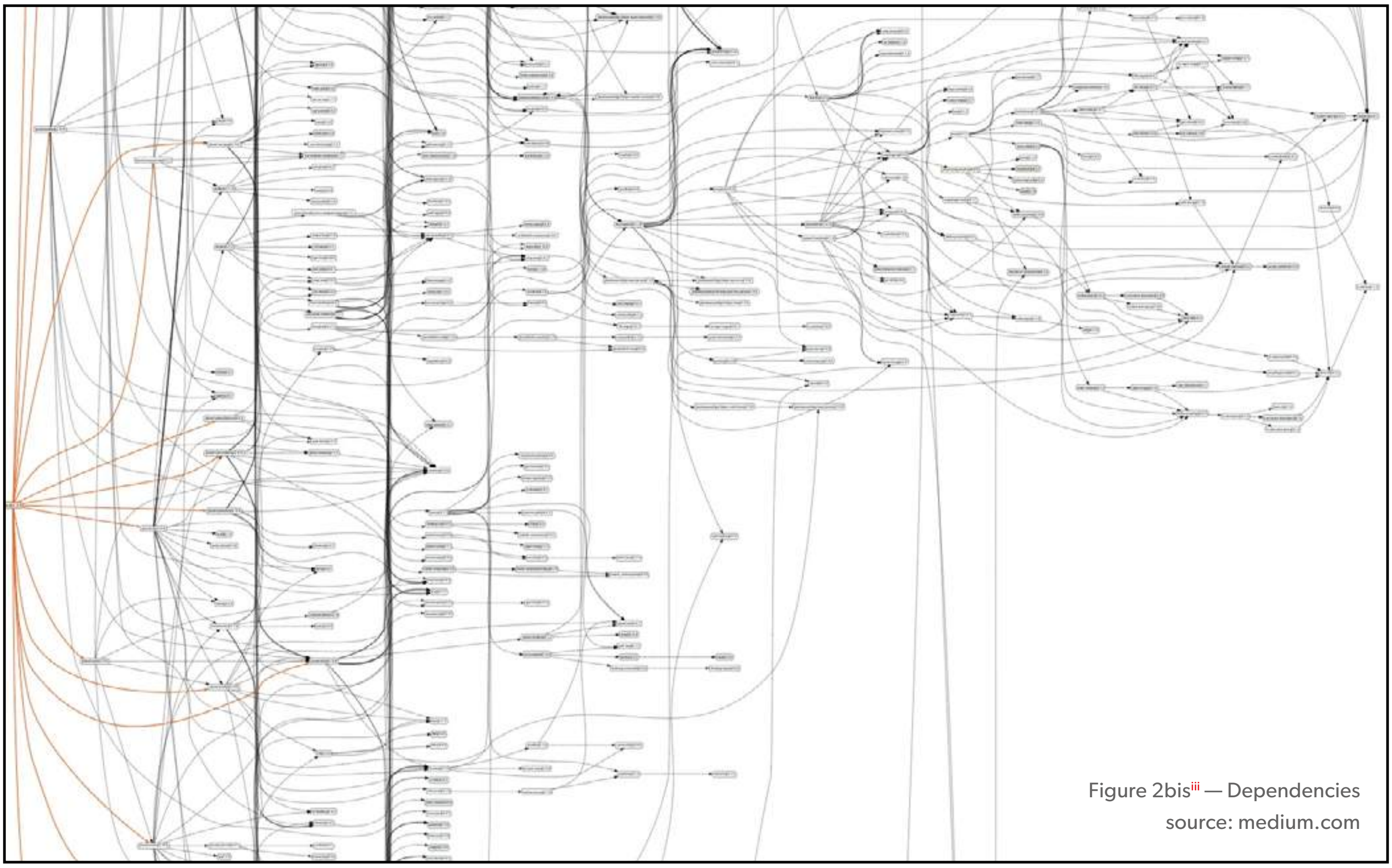


Figure 2bis[iii] — Dependencies
source: medium.com

Complexity, resilience and freedom to action

BOX 2

One of the most challenging features of today's digital infrastructures is their increasing complexity.

Herbert Simon was among the first to study "complex systems". In 1962 he wrote a seminal article on their properties. Simon set out to explain why complex systems frequently take the form of hierarchies with sub-systems are "nearly-decomposable." By this, he means that there is more interaction within a sub-system than between sub-systems, so they are relatively independent. According to Simon, a kind of natural selection favours these architectures over time and over the course of evolution over tightly integrated systems. These structures better withstand stress, unexpected changes, and accidents, and are able to recover more quickly and restart in better condition after a crisis and failure (Simon, 1962).

In current language, we would say that complex systems have a tendency to organise themselves in a layered and modular way. Today, we use the term "resilience" for the characteristics cited by Simon.

Most complex systems incorporate this architecture, and the main underlying reason is superior **resilience**. In complex systems - so in today's digital systems - resilience has a rewarding and primary value over other organisational principles.

Iochai Benkler, one of the leading contemporary scholars of digital commons, also reached a similar conclusion. Benkler has devoted much of his work to explaining the success of a non-proprietary model - such as Free and Open-Source Software - in digital technologies and systems. The main explanation, according to Benkler, lies in the conditions of continuous change and uncertainty, and "error-prone systems", as are the systems characterised by continuous change and uncertainty.

These conditions – which are those of modern digital technological systems - impose maximum **freedom to operate**. Digital commons often prevail because, given certain conditions, they offer superior flexibility, eliminate transaction and negotiation costs (no contracts or permits are needed), and make the cost of exploration and failure much cheaper. The freedom to operate is thus the supreme value, even with respect to optimisation, control by exclusive property, and the possibility of direct appropriation of the technology's value (Benkler, 2013).

These arguments are even more important since there seems to be an unstoppable trend toward an increase in the scale and complexity of digital systems. One of the reasons is digitisation itself. The more the world is digitised, the more interconnected it becomes. The more systems become integrated, the more complex they become. New terms have been coined to describe these systems, such as, "Ultra-large-scale systems" (Northrop & al., 2006) or "Large-scale complex IT systems" (Sommerville & al., 2012). The emphasis is often placed on the unprecedented scale, their characteristic volume of hardware, code, users, and data, the complexity of independent components and the continuously changing sub-systems of which they are composed. But the idea is also that this scale and complexity comes with characteristics that challenge traditional approaches to engineering, management and governance. The absence of centralised control, the **polycentric** nature (Ostrom, 2010), and the constant evolution of these systems, subsystems and components makes **failures a norm** and not the exception. This puts pressure on the governance of these systems, especially in conditions of interoperability and interconnectedness, which must also continually evolve (Rezaei & al., 2014).

2

IS THERE A EUROPEAN WAY TO CLOUD COMPUTING?

2.0

THE SHIFT IN THE EUROPEAN APPROACH TO DIGITAL POLICY

We are therefore in a crucial passage in the development of the digital revolution. This explains the race to accelerate the adoption of cloud technologies – and the fear of deepening technological dependence.

Indeed, the European Union long ago identified the importance of this transition. In a 2012 Communication Unleashing the Potential of Cloud Computing (European Commission, 2012), the EU Commission even tried to outline a strategy to achieve European technological and industrial "leadership" in this transition. The The lack of results sounds alarming, in view of the stated renewed ambitions.

According to a recent analysis, the the European cloud infrastructure services market, is now five times as big as it was back in 2017.

The collective market share of the European players on this market, however, has shrunk from 27% to a mere 13% (see Figure 3), with the global public cloud infrastructure market converging around three large USA corporations (Synergy, 2022).[iv]

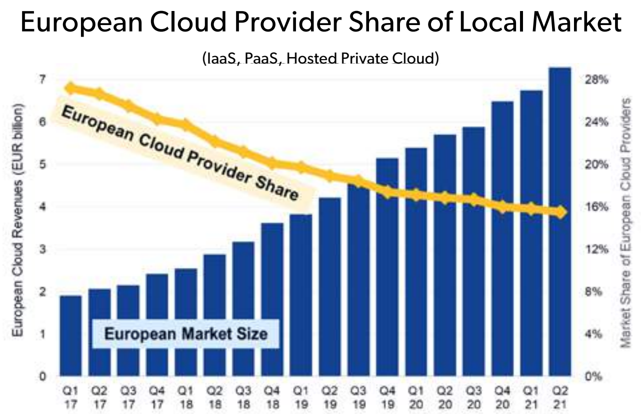


Figure 3 — source: Synergy Research Group

The strongest European cloud players are SAP and Deutsche Telekom (each of them with a mere 2% of the European market share), followed by OVHcloud, Telecom Italia, and Orange (Martí, 2022).

Furthermore, apart from the French exception, which has, however, racked up quite a few failures, the construction of an autonomous industry in the digital domain has never really entered the agenda at European level, at least until very recently. Behind this absence of industrial policy, there have been divisions and disparate economic interests between different countries and governments. But above all the main obstacle has been the general consensus in favour of neoliberal policies, which have prescribed government abstention from intervention in technological development and industrial policies.

This orientation has undergone a gradual progressive rethink. There have been many reasons for this in the digital field.

2.1

PROTECTION FROM THE US SURVEILLANCE COMPLEX

The first steps were motivated by political factors. Edward Snowden's revelations in 2013 about the use of pervasive surveillance on Europeans and their political leaderships by the US National Security Agency (NSA) through communication networks and US digital monopolies brought to light what has recently been called the "Surveillance Industrial Complex" even in the USA itself.

Snowden's revelations provoked strong reactions, especially in Germany. Combined with the growing alarm caused by the rise of "surveillance capitalism" (Zuboff, 2019) and the uncontrolled use of personal data by companies at the forefront of digital capitalism, these concerns led to the first real European regulation in the digital age: the **General Data Protection Regulation** (GDPR), the first worldwide legislation to regulate the use of personal data. This regulation was fairly light-touch, but still had to overcome fiery resistance from the "formidable alliance of Big Tech, the US Congress, and the Obama administration" (Barker, 2010). Despite many detractors and not a few ironies, the GDPR quickly produced two largely unexpected results.

First, it has become a worldwide standard. This is because other governments have taken the European regulation as a model (including, for example, the State of California, which introduced a state law in the face of the US federal government's refusal to introduce privacy protection regulations). Because large global companies have adopted the GDPR as a standard rule to streamline their operations across multiple jurisdictions. The EU - an entity of 450 million inhabitants and one of the world's largest markets - has thus tested its regulatory power.

This is the so-called **Brussels effect** (Bradford, 2012). The second consequence has been the use that citizens' digital activism has made of the regulation, leading it to achieve results that legislators had not imagined. This is what happened with the two rulings by the Court of Justice of the European Union (CJEU) known as **Schrems 1** and **Schrems 2** (see Box 1), because of the name of the Austrian digital activist who prompted them. These rulings declared transfers of personal data from the EU to the US illegal, as they do not guarantee protection of European citizens from US agencies surveillance activities. This potentially wreaks great havoc on the business models of large US companies and could lay a foundation stone for what has later become the doctrine of "European digital sovereignty" in the domain of data. The game is not over, however.

In fact, the European Commission has clearly shown that it has no intention of following through on this line. In July 2023, just few weeks after a heavy penalty imposed on Facebook confirmed the illegal nature of these personal data transfers in the US, it made executive a new legal framework for allowing transatlantic data flows , based on an agreement signed between Biden and Von der Leyen in May 2022, in the immediate aftermath of the Russian invasion of Ukraine. Nevertheless, in spite of improvements, the new Trans-Atlantic Privacy Framework is again going to be challenged at the CJEU by Schrems and other associations defending citizens' privacy rights.

The battle for the "sovereignty" on personal data — BOX 3

Much of the progress in the defence of European citizens' rights against the pervasive surveillance practices of US companies and government security agencies is due to the stubborn battles of an Austrian activist and lawyer: Max Screms. His lawsuits resulted in two rulings by the Court of Justice of the European Union (CJEU) which destabilised the routinary transfers of EU citizens' personal data to the United States. The US laws, the Court ruled, did not offer the privacy protection established by the GDPR - and European citizens do not have adequate legal tools to assert their rights in the USA. The Court also declared invalid the Safe Harbour Principles, an agreement stipulated by the Commission in 2000 on the basis of which large US technology companies were able to transfer the personal data of European citizens to the USA; and in the second ruling, it extended this judgment of inadequacy to the "standard contractual clauses" used by US companies, which previously enjoyed a presumption of validity.

The Court explicitly stated that these regimes did not offer guarantees that once EU citizens' personal data has been transferred across the Atlantic it will not be accessed by US intelligence agencies. The problem is that US security agencies maintain the practice of massively collecting data, sometimes even simply by purchasing it from Big Tech companies (Cameron, 2023).

The Battle of Schrems began over ten years ago. Already in 2013, he filed a complaint against Facebook Ireland Ltd., i.e. the European headquarters of Facebook (now Meta). At the time, the GDPR had not yet been approved (it would be approved in 2016 and came into force in 2018) and the main legal shield used by Schrems was the Charter of Fundamental Rights of the European Union (approved in 2007), especially Article 8 on the protection of personal data. In Europe, the practice of transferring data to the USA was based on a decision of the European Commission, taken in 2000, known as the EU–US Safe Harbour Principles, which effectively allowed the unrestricted transfer of data and personal information from the EU to the USA.

Given Edward Snowden's revelations in 2013 and the alleged involvement of Facebook USA in the PRISM mass surveillance programme, Schrems argued that the application of the Safe Harbour system violated his personal fundamental right to privacy, data protection and to a fair trial, guaranteed by the Charter of Fundamental Rights of the European Union. In the first instance, the application was rejected by the Ireland Data Protection Commission (DPC) - the Irish national independent authority responsible for upholding the fundamental rights of individuals - saying that it was "frivolous and vexatious".

This led to a request for judgment from the Irish High Court, which in turn suspended the judgment by consulting the Court of Justice of the European Union (CJEU), on the adequacy of the European directives in force. Finally, on 6 October 2015, the Court of Justice of the European Union ruled that the Safe Harbour framework was invalid for several reasons: it allowed government interference, it did not offer legal remedies for European citizens who want to access or delete or correct data relating to themselves, and it stops privacy protection authorities from supervising the processing of their personal data. It moreover declared illegal the data-sharing rules with countries that have lower privacy protection standards than those of the EU, including the USA.

As soon as the GDPR came into force, Schrems again launched new actions against many companies, including Google, Amazon, Apple Music and others. A new CJEU judgment (Schrems II) in 2020 again ruled that European data-protection authorities must stop transfers of personal data. Despite these rulings, however, major US companies have avoided applying them, and continued to transfer European citizens' data. They have been playing on the slowness of judicial systems and have been working in parallel with the US government to reach a new agreement with European authorities that could avoid the application of those rulings. To understand how strategic these issues are - and how high they are on the US government's agenda - it is significant that in Brussels in March 2022, Biden and Von der Leyen used their first meeting following the Russian invasion of Ukraine to reach the new agreement: the EU-US Data Privacy Framework.

The new agreement was then formalised in 2023. According to the Commission, the agreement addresses all the points raised by the EU Court of Justice, limiting access to EU data by US intelligence services to what is "necessary and proportionate" to protect national security, and establishing a Data Protection Review Court to resolve European citizens' allegations of unlawful access to their personal data. However, the battle is far from over. Despite improvements, the new agreement is again going to be challenged by Schrems and other civic associations at the CJEU. They consider the new agreement inadequate mainly for two reasons: the lack of US legislation on the protection of privacy, such as would provide the same guarantees as GDPR, and the inadequate guarantees provided by the US administrative court to which EU citizens should take recourse to protect their rights.

2.2

CHINA'S RISE AND THE TECHNOLOGICAL CLASH WITH US

Yet there were also other considerations which paved the way for the shift in European digital policies. One critical factor was China's surprisingly rapid rise on the frontiers of technological innovation.

Its technological-industrial development model - although it would be simplistic to call it *dirigiste* and statist (Heilmann, 2009; Lin, 2011; Heilmann & Melton, 2013; Jin, 2023) - has certainly made massive and effective use of governmental industrial and technological policy. This is, moreover, a recipe common to all Asian countries (World Bank, 2008).

This rise and the shock caused by Huawei's leadership in 5G have played a fundamental role in transforming the orientation of technology and industrial policy in Europe. Still, their effect has been even more disruptive in the United States.

In the space of just a few years, it has caused a radical reversal of US policies: the abandonment of the Washington Consensus (Williamson, 1990; Sullivan, 2023a), the assertion of geopolitical over commercial primacy in technology, and the adoption of protectionist industrial policy in most advanced technologies in the attempt to hamper and contain China's rise.

For Europe, this has further complicated the situation, as it meant being dragged into a "**technological war**" between the United States and China, with the real risk of a decoupling between the US and Chinese technology ecosystems, without Europe being able to articulate an autonomous strategy of its own. The result has been a perception of vulnerability and dependence, which has been amplified and dramatised by the pandemic and the need to rely on online and digital solutions for education, work and essential services.

Distribution of Top 100 Digital Platforms by Market Capitalization, 2021

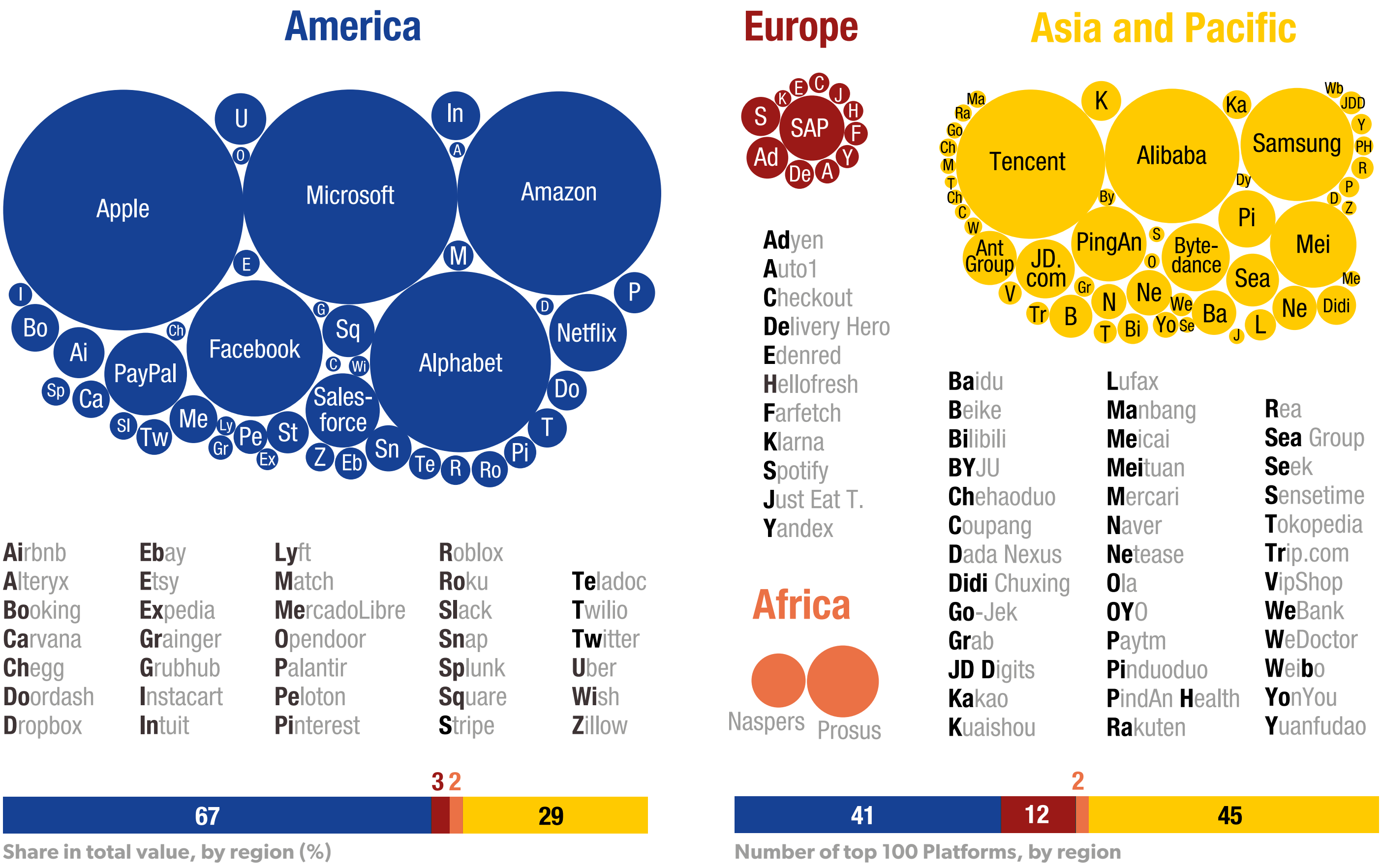


Figure 4 — source: UNCTAD Digital Economy Report 2021, Holger Schmidt, available at netzoekonom.de | Note: As a reference, the market capitalization of Apple is $2.22 trillion, while for Mercado Libre it is $88.7 billion, $80.2 billion for Baidu and $59.7 billion for Spotify.

2.3

HUGE AND EXPANSIVE MONOPOLIES

A further factor has been the abnormal growth in the power and wealth of the large monopolies that have established themselves in the digital domain. Its most impressive expression has been the growth over the last ten years in the capitalisation of companies such as **Apple**, **Microsoft**, **Google**,**Amazon and Meta**. Behind this spectacular growth are monopolistic profits and the proven ability of these companies to expand into new sectors, through acquisitions and now unbridgeable advantages in transversal assets - such as data, infrastructure, commercial networks, and know-how - which allow economies of scale and scope in different and distant areas and sectors. These unbridgeable advantages of course also include their financial capacities, which stock market valuations have magnified (see Figure 4). Consider that between 2011 and 2021, Apple, Google, Amazon, Meta, and Microsoft made hundreds of acquisitions to expand into new areas or to eliminate potential competitors, and that Big Tech spends $150-200 billion annually on research and development (see Figure 4bis). In comparison, Horizon Europe, the EU research programme for 2021-2027, has a total budget of €95.5 billion. Moreover, to complete the *cahier de doléances* of European governments on this issue, Europe suffers from massive tax avoidance by these same companies. At the same time, faced with this sprawling growth, traditional anti-trust instruments and doctrines have proved outdated, slow and completely ineffective.

R&D of Top Tech Companies in 2022

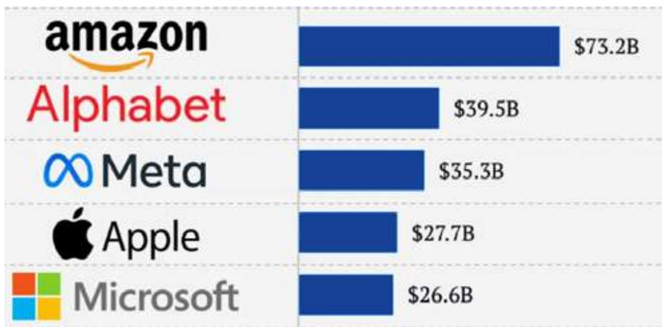


Figure 4bis — source: Stockanalysis.com

2.4

THE ROLE OF DATA IN FUTURE ECONOMY

A final factor has arisen to exacerbate this situation: the growing awareness of the central importance of data in the advancement of the latest generation of technologies and in the transformation of **future value chains** in all economic sectors. This thus also affects more traditional industrial sectors, in which Europe - and Germany in particular - still have a strong and leading position. The inability to convert this conventional industrial strength into a leadership in digital transformation and the loss of control over data in these same activities has begun to be seen as a fatal risk of losing the main opportunities for innovation and value-added services in these sectors in the future. The danger is that US (or Chinese) Big Tech will take advantage of their dominant position, especially on data and AI algorithms, to carve out the lion's share in these new markets.

3.0

A MULTIPLICITY OF INITIATIVES IN CLOUD COMPUTING

Hence by the time of the 2019 European elections and the arrival of the new Commission, the conditions were ripe for a turnaround in European digital policies.

The main sign of a change in the EU's orientation is undoubtedly the proliferation of legislative initiatives. Between 2019 and 2023, 18 regulations and directives in matters related to digital policy were approved or proposed, 15 of which have a direct relevance to cloud computing (see Figure 5). (Those dating from 2019 are the result of work that had already begun during the previous Commission).

The reluctance or fear over intervening with regulations is clearly water under the bridge. Rather, the difficulty lies in navigating this sea of regulations, which add up to hundreds of pages and articles of law. Moreover, many of these regulations return time and again to the same topics, which partly reflects the uncertainties and evolving approach of EU legislators, which is coupled with the difficulty of legislating in such a dynamic field of continuous innovation. Quite a few observers see this intense legislative activity as an additional burden on small businesses and innovators in the EU. On the other hand, European legislators defend it as a useful tool – not only to protect citizens' rights, European values and fair competition, but also to strategically direct and guide investments and research in the EU and to influence global digital markets towards European-defined legal and technical standards.

Regulations & Directives 2019-2023

Approved

Cybersecurity Act	2019
Platform to Business Practices	2019
Copyright in the Digital Single Market	2019
NIS 2 Directive	2022
Data Governance Act (DGA)	2022
Digital Operational Resilience Act (DORA)	2022
Digital Makets Act	2022
Digital Services Act	2022
Critical Entities Resilience Directive (CER)	2023

Proposed

European Health Data Space (EHDS)	2022
European Data Act	2022
Cyber Resilience Act (CRA)	2022
Interoperable Europe Act	2022
Standard Essential Patents	2023
Artificial Intelligence Act	2023

Figure 5

These legislative initiatives have been accompanied by an equally important effort in the form of a multitude of policy statements (see Figure 6) and initiatives. The subject of cloud computing features in many such initiatives, regulatory or otherwise. In some cases, it is one of the central themes. In others, it is an integral element, as an essential infrastructure that cuts across all sectors.

Faced with this dispersion and stratification of interventions and regulations, cloud providers in the EU are keenly awaiting a document on which the Commission has been working since 2021, namely the **Cloud Rulebook**. It should summarise and give order to the set of norms, standards, recommendations and guidelines, which have progressively accumulated around cloud computing (see Box 4). But this cannot be published until the issue of the EUCS - Cybersecurity Certification Scheme for Cloud Services - currently under discussion at ENISA - European Union Agency for Cybersecurity - is resolved (see Box 6).

Main EU strategic statements

Building the next generation cloud for businesses and the public sector in the EU	Declaration EU Council	2020
Berlin declaration on Digital Society and Value-Based Digital Government	Declaration EU Council	2020
European data strategy	Strategy EU Commission	2020
EU's Digital Decade	Strategy EU Commission	2020

Figure 6

The Cloud Rulebook

BOX 4

The EU Cloud Rulebook is a long-awaited EC document that is expected to summarise the set of legislative and non-legislative regulations, including self-regulatory standards, on security, energy efficiency, data protection, interoperability and fair competition in cloud computing. These regulations and certifications include the **EUCS** - the EU-wide cloud cybersecurity certification scheme - currently being discussed within ENISA (see Box 4).

The EUCS, initially announced for 2021, is still under discussion. Another example of regulation that the Cloud Rulebook should contain are the **SWIPO** codes of conduct on data portability in the cloud. These are voluntary codes of conduct required by the free flow of non-personal data regulation passed in 2018, which have been defined by the cloud industry providers and users stakeholders in 2020, under the supervision of the European Commission. In theory, they should make it easy to migrate data and applications from one provider to another, avoid "vendor lock-in" and facilitate switching between providers.

Other examples of regulation are the **Standard Contractual Clauses**, for instance relating to service levels or data protection, which should help reduce asymmetries in bargaining power between providers and users-customers; and the **Code of Conduct** on the energy efficiency of data centres, which should (also through public procurement) promote the adoption of energy efficiency codes in data centres, and initiatives aimed at making them "climate-neutral."

⇢ 3.1

A GLOBAL STANDARD SETTER FOR REGULATION

With all this normative activity, as a legislator the European Union has become a pioneering laboratory for digital regulation. Indeed, it makes no secret of the fact that it aspires to influence global regulatory standards on emerging digital technologies.

Laws such as the Digital Market Act (DMA) and the Digital Services Act (DSA), which regulate the platforms and gatekeepers of the digital economy (see Box 5), or the long-awaited AI act, are regulations that are bound to have a global impact and influence.

Regulating platforms and gatekeepers

BOX 5

The so-called package of digital services regulations passed in 2022 includes two regulations, the Digital Services Act (DSA) and the Digital Markets Act (DMA), which aim to protect users' basic rights and establish a more level playing field for businesses. Both regulations must be associated with the recognition of the infrastructural function that digital platforms perform, namely the provision of essential services such as utilities.

Historically, infrastructures have commonly been considered as unsuitable for being provided and managed by a pure market logic. They have instead been associated with some kind of public intervention, either through direct control and ownership or through regulation, in order to ensure the cheapest, most universal and non-discriminatory access possible to both market actors and citizens (Frischmann, 2012). Moreover, these essential systems of general utility, especially when provided by networked infrastructures, tend to benefit from network effects and generate monopoly or quasi-monopoly conditions, thus providing a potential exorbitant power over the entire universe of activities (Rose, 1986; Berlinguer, 2021). This is the case with the "gatekeepers", a special category of platforms and essential infrastructures which is tackled by the Digital Markets Act.

Specifically, the **Digital Services Act** regulates online intermediaries and platforms. The main DSA objectives are to free users and business ecosystems from private, nontransparent and unchecked rule; to introduce a regime of content moderation; to limit targeted ads; and to push towards transparency on algorithmic content moderation and prioritisation.

The **Digital Markets Act**, for its part, introduces new rules that govern the "gatekeepers": the very big online platforms that have a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services. The DMA covers eight sectors named "Core Platforms Services": online search engines; online intermediation services; social networks; video sharing platforms; communication platforms; advertising services; operating systems; and cloud services. Gatekeepers are defined according to objective criteria related to the number of users (45 million monthly active users and at least 10,000 yearly active business users in the EU), turnover (at least €7.5 billion in each of the last three financial years) or capitalisation (at least €75 billion).

For these companies and products, the Digital Markets Act establishes specific obligations and prohibitions, such as the obligation to allow third parties to interoperate with the gatekeeper's own services; to allow business users to access the data that they generate; to allow companies doing advertising to carry out their own independent verification; and to allow business users to promote and sell their products outside the gatekeeper's platform. Prohibitions include those of preventing users from uninstalling preinstalled software and treating products offered by the gatekeeper more favourably in rankings.

Fines can reach up to 10% of the company's total worldwide annual turnover. So far, six companies have been registered as gatekeepers for specific products: Apple (for Safari, iOS, App Sore), Microsoft (for LinkedIn and Windows), Amazon (for Amazon ads and Marketplace), Meta (for Facebook, Instagram, WhatsApp, Messenger, Meta Marketplace and Meta ads), Alphabet (for Google Maps, Google Shopping, YouTube, Chrome, Android, Ads, Google Search, and Google Play) and ByteDance (for TikTok).

This regulatory goal is also intertwined with the ambition to set standards for technology, which should incorporate these same regulatory principles in emerging areas such as AI, IoT, Edge-Cloud computing, or Cybersecurity. Indeed, the ambition to use standards in combination with internal market dimensions as a tool of industrial policy has long been present in EU policy (European Commission, 2013; European Commission, 2016).

On cloud computing, however, the introduction of systems of control and certification of the legal and technical characteristics of digital services is the focus of many European regulations and initiatives. Gaia-X - a project born in 2020 from an initiative of the German and French governments, which was presented as a linchpin of these new European aspirations to digital sovereignty - has progressively centred on the construction of a technological framework that should standardise, operationalise and automatise these certified controls (see Box 8).

3.2

DIGITAL SOVEREIGNTY

As we have said, it is not easy to navigate our way through this multitude of initiatives. But if we had to choose a single term to sum up all the EU initiatives, the main watchword would have to be "**digital sovereignty**". This idea has become a central guiding principle for Europe's engagement in digital and technological affairs since 2020. The concept has during the 2020s been affirmed in a series of documents and declarations by the Parliament, the European Commission and the European Council.

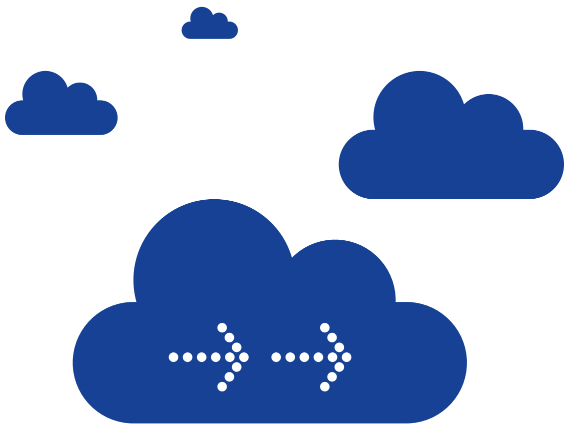
Most importantly, the concept has been endorsed in a European Council declaration: the Berlin Declaration on Digital Society and Values-Based Digital Government, in 2020 during the German Presidency of the EU, which represented a watershed moment in EU digital policy. The Commission has made digital autonomy a central point of its programmes. The European Parliament has generally shown a clear support for the principles of digital sovereignty and, if anything, a favourable inclination towards more stringent measures, compared to the Council and the Commission.

However, there are at least **two** possible **interpretations** of digital sovereignty in the formulations which have been used. The first expresses a determination to reaffirm the Westphalian concept of an exclusive monopoly of legitimate **regulatory power** within one's own borders, albeit adapted to Europe's politically complex context of shared sovereignty, and to a global and digital age. The second, on the other hand, emphasises the preservation of autonomy and self-determination in the face of dependence on critical digital systems: that is, the maintenance of conditions that allow **freedom of choice and action** for individuals, organisations and governments in relation to their digital interactions, their data, and their dependence on complex technological systems.

Regarding the first meaning, the articulation of a common digital sovereignty in Europe is a complex path, as each state maintains its own sovereignty in many of the most critical areas.

n this respect, cybersecurity can be seen as very much a laboratory. And the EU is proceeding quite slowly and only step by step. In fact, many EU's regulations in the digital sphere revolve around the issue of security and already in 2017, ENISA - the European Union Agency for Cybersecurity - was created with the aim of building a common framework shared by the different national cybersecurity agencies and fostering greater European coordination. Right now, as mentioned, ENISA is indeed at the centre of one of the main areas of tension and negotiation with the US. It is focused on the definition of a European Cloud Security Certification Scheme - the **EUCS** (see Box 6) - and tensions particularly revolve around the so-called "**sovereign clauses**", which are meant to certify that Cloud Service Providers (CSP) do indeed guarantee data security from interference by non-European authorities and jurisdictions.

US technology companies and the US government see these clauses as a threat and a protectionist move. In fact, although the ENISA certification scheme is a voluntary framework, these clauses could become a lever to exclude US and Chinese suppliers, at least in the essential services that are regulated by the new NIS2 directive and in which EUCS could become mandatory.



EUCS sovereign clauses: to be or not to be?

BOX 6

The EU's ambitions of sovereignty seem to be caught up in a long debate about the so-called EUCS. The acronym stands for "EU Cybersecurity Certification Scheme for Cloud Services." Initially announced for 2021, the EUCS is still under discussion. The scheme is supposed to certify legal guarantees and security, uniformly within the European Union, on the base of a catalogue of security levels appropriate to the different types of services and data, both for enterprises and public organisations..

The EUCS has been under discussion within ENISA, the European agency responsible for cybersecurity, since 2020. ENISA is supposed to release a series of labels for different levels of certification of the characteristics and security of cloud services. These labels are the focus of multiple expectations and pressures. The heart of the discussion centres around the so-called "sovereign clauses" which should apply to the most sensitive data. These sovereign clauses are certifications and requirements that the French cybersecurity agency has already approved in its certification system, SecNumCloud, and which the French government is pushing to extend to the scheme under discussion at ENISA.

These certifications should guarantee that the cloud services offered are immune from foreign laws and authorities. For this purpose, they are meant to ensure the localisation of cloud services and data in Europe, but also exclude companies subject to non-European legislation, because these latter could be obliged by laws, such as the Cloud Act approved in 2016 in the USA, to make public administrations' and European citizens' most sensitive data accessible to foreign authorities and intelligence systems, even when it is stored in data centres in Europe. Although ENISA requirements and certifications will be classified as voluntary, the expectation is that through the revision of regulations on the security of critical infrastructures and entities, these requirements may become mandatory in some areas, in particular through the revision of the Directive on Security of Network and Information Systems (NIS).

The new version - NIS2 - will require compliance certification for the IT components of these infrastructures. In this way, North American and Chinese cloud providers could be excluded from public tenders and from the provision of services for critical infrastructures. The main US tech industry lobbies are exerting great pressure against the sovereign clauses.[v] And a group of 7 governments – Denmark, Estonia, Greece, Ireland, the Netherlands, Poland, and Sweden – raised objections to these clauses.[vi] In the European Parliament, however, a cross-party group was formed to support the French proposal. As far as is known, France is the main promoter of their inclusion at the European level and is supported by the governments of Italy and Spain, whereas the new German government declared itself in favour of a political discussion on the topic.

However, the concept of sovereignty, as mentioned, is also articulated in European documents as a guiding principle called upon to safeguard autonomy, freedom of choice, and the ability to act and change technological systems in the new digital environments. This is perhaps its most innovative meaning.

This concept is, indeed, reflected in many different norms. These include the battle against monopolies and the obstacles they pose to innovation and choice - for example, with the imposition of binding **interoperability** rules on the "gatekeepers" in what the Digital Market Act has defined as "core platform services". It is also reflected in the demand for **transparency** on the use of data and algorithms in the AI Act.

Equally, in the regulations, such as the Data Act and the Data Governance Act, that aim to guarantee self-determination and control over one's own data. But perhaps the most peculiar application is in the delineation of a federated, modular and open-source **matrix** that should guide the design of the **architectures of** cloud computing and **digital systems** more generally. We shall return in the last part to this matrix of principles of technological design, as first outlined in the Berlin Declaration of 2020, in a chapter entitled "Digital sovereignty and interoperability" with specific reference to cloud computing used by the public sector (EU Council, 2020b).

In the meantime, it is interesting to note the association that this notion of sovereignty establishes between certain principles of technological design - in particular modularity, open source, interoperability, and standards - and the safeguarding of values such as freedom of action and innovation.

3.3

THE EUROPEAN DATA STRATEGY: TRUST AND LEGAL CERTAINTY AS COMPETITIVE ADVANTAGES

Again, in trying to extract an underlying rationale, three guiding principles can be identified in the EU's initiatives that seek to influence the evolution of digital systems in cloud computing. These include ensuring compliance with EU laws, guaranteeing user rights and security; a parallel pursuit and demand for transparency; and a gradual attempt to disarticulate closed, opaque and centralised systems, such as those that currently predominate in cloud computing.

But in terms of our own greatest interests here, what is the industrial strategy for cloud computing? In a nutshell, the stated goal is to support the formation of a **common European "federated infrastructure"** based on common standards and interoperability principles, which should avoid lock-in and ensure secure data management, and which should at the same time move toward the next Edge computing-oriented architecture.

The **European Data Strategy** 2020 is one of the most important policy documents in which these strategic axes have been defined by the EU Commission. In it, **Edge computing and "industrial" data** are identified as the two main innovation opportunities for European industry. Research funding programmes have also at least partly been oriented in service of this strategy. Horizon Europe - the EU's research programme - has been pulled in the direction of projects consistent with the EU's strategic objectives in the digital sphere, promoting large-scale cooperation between European players and influencing technological development.

On industrial data, the EU aspires to build a leading ecosystem of innovation based on its strength in traditional manufacturing, which potentially provides a rich source of strategic data for the development of future services. At the same time, leveraging its leadership in regulation, the EU aims to set out a competitive context based on its guarantees of transparency, legal certainty and rights protection. This is meant to provide reassurances to overcome the main barrier to cloud adoption and data exploitation, i.e. the lack of trust among companies, citizens and institutions.

In the regulatory domain, the foundations on data regulation were laid in the previous legislature, for personal data with the GDPR (in 2016, entering into force in 2018), and with the Regulation on the Free Flow of Non-Personal Data (2018). During this term of the EU parliament, new legal and regulatory instruments were added to these foundations, with the Data Act and the Data Governance Act, which mainly intend to enhance and regulate the access and use of personal and non-personal data by innovators (see Box 7).

The overall goal is to make the EU a legal and economic area predisposed to facilitating experiments and innovations in the use of either personal or non-personal data, while making legal security and the trustworthy nature of regulation, guarantees and infrastructures - also on the technological terrain - the EU's brand and competitive advantage.

The EU data strategy

BOX 7

The "data strategy", presented in 2020, has been at the heart of the new European digital policy from the outset. The declared ambition is to make the EU a leader in the future "data-driven society". And EU data legislation is undoubtedly the most prolific and extensive in the world.

The issue of data pervades all sectors of the digital economy and is thus present in all digital regulation. However, there are six specific regulations focused on data. The first foundations were laid in the previous legislature with the General Data Protection Regulation (2016) which regulates the use of personal data and with the Free Flow of Non-Personal Data (2018) for non-personal data, aimed at liberalising the flow of data within the EU.

Meanwhile, the Open Data Directive (2019) replaced the Public Sector Information (PSI) Directive, with the aim of promoting access and re-use of data held by public institutions. In this legislature, three new legislative initiatives have been added (of which only the first has been definitively approved): the Data Governance Act, the Data Act and the European Health Data Space.

All these regulations centrally aim at incentivising and facilitating the economic, scientific and technological exploitation of data.

The **Data Governance Act** (DGA) has among its main objectives to increase the availability of data by creating legal certainty, especially by clarifying users' ownership of the data generated when using products and services. This is intended to incentivise manufacturers to invest in high-quality data generation and encourage more players to participate in the data economy.

One of the main innovations introduced by the DGA is the promotion of common European data spaces in strategic sectors such as public administration, health, environment, energy, agriculture, mobility, finance, and manufacturing. The complex and ambitious goal is to create a federated community of "sovereign data ecosystems", based on cross-sector common cloud, data, and AI infrastructures.

Other objectives of DGA encompass several issues, including: reducing barriers to the reuse of data, including public sector data that cannot be made available as open data; regulating data intermediaries as trustworthy facilitators of data sharing, data pooling and data markets within the common European data spaces; and facilitating and increase trust in "data altruism", encouraging voluntary data sharing.

The **Data Act** is a regulation proposed by the EU Commission in 2022. It aims at addressing the legal, economic and technical issues that lead to data being underused, by defining new rights for users of connected devices to access and share the data that they generate through their use. It has specific provisions addressing the Internet of Things (IoT), and cloud services providers, including by introducing rules to facilitate access to and portability of data and switching between cloud providers, and by setting rules on switching charges and addressing the absence of technical tools, standards and technical **specifications for data portability and interoperability** among cloud providers.

The regulation stipulates the introduction of a binding obligation for cloud service providers to offer data and application portability, although according to the proposal these requirements only apply to infrastructure-as-a-service (Iaas), the most basic layer of computing services, and to raw data. The European Data Innovation Board (created by the DGA) should assist the Commission in defining interoperability specifications and standards. These essential requirements on interoperability should apply to the EU common data spaces. The Commission will also develop model contract clauses to prevent abuse of contractual imbalances. The regulation should also introduce ways for public sector bodies to access and use data held by the private sector that is necessary for purposes of public interest.

Healthcare is one of the sectors expected to be most affected by digital transformation and data exploitation - and it is also where the European Commission has proposed the first sectoral legislation on data: the **European Health Data Space** (EHDS). The EHDS sets out the rights of individuals to access and control personal health data and aims at creating legal clarity and a trustworthy governance to encourage voluntary data-sharing to third parties, with data anonymising or aggregating rules, for the use of health data for research, innovation, policy-making and regulatory activities. At the technological level, the EHDS is set to establish a dedicated and common digital infrastructure (MyHealth@EU), for the governance of the European Health Data Space, based on common rules, standards and cross-border interoperability requirements.

3.4

A FEDERATED FRAMEWORK FOR CONTINUUM COMPUTING

The EU's other bet is on edge computing. The evolution towards a federated infrastructure of continuum computing is functional to **"industrial" applications** on data use. But it is also seen as a new technological framework that should help to disarticulate the hypercentralised and closed architectures of the dominant cloud providers, through the imposition - also for technological needs - of open standards and interoperability principles.

To support the growth of an autonomous digital industry, the EU is also actively promoting the creation of **collaborative ecosystems**, both in edge-cloud computing and in data exploitation strategies. This seems to be possibly one of the most difficult undertakings for Europeans, as EU countries cannot rely on big digital platform companies, like the USA and China. This requires the invention of alternative collaborative strategies whose success relies on coalescing disparate interests across countries and sectors.

With regard to data, the most important organisational innovation that has been devised thus far is the promotion of "**data spaces**". This means common European spaces in crucial economic sectors and areas of public interest, where innovative forms of data sharing and commercial use should be incubated and tested, and around which common technological infrastructure, standards and interoperability rules should take shape. In healthcare - considered one of the most promising and critical sectors - a specific legislation, the European Health Dataspace, has also been proposed.

In the area of edge-cloud technologies, the main initiatives are two public-private partnerships: the **Alliance for Industrial Data, Edge & Cloud** and an IPCEI (**Important Project of Common European Interest**) **on Next Generation Cloud Infrastructure and Services** (see Box 8). The IPCEI is an instrument provided for in the European Treaties since 1957, which allows the possibility of granting state aid under certain conditions, but it has long remained virtually unused.

IIn 2020, the governments of Germany and France proposed an IPCEI on next-generation cloud infrastructure and services, and in 2021 the European Commission approved a general regulation on IPCEIs (European Commission, 2021). This latter is mainly concerned with defining the rules for justifying IPCEIs (based on the highly innovative nature of projects and the existence of market failures due to the high risks involved), their governance, transparency in public funds, limiting internal competition distortions, ensuring positive spillovers for non-participating companies and users throughout Europe, and the introduction of a claw-back mechanism, whereby, in the event of successful projects, beneficiary companies are required to repay part of the aid received (European Commission, 2021).

The IPCEI-CIS on next-generation cloud infrastructure and services was finally approved in December 2023 as a project sponsored by the governments of France, Germany, Hungary, Italy, the Netherlands, Poland and Spain, which together will provide €1.2 billion in public funding.[vii]

A constellation of initiatives on the cloud

BOX 8

Below we briefly present the most significant projects undertaken by either the European Commission or by major European governments in the area of cloud computing in recent years, with the ambition of promoting and directing the development of cloud infrastructure and technical solutions for cloud and industrial exploitation of data.

Gaia-X[viii]

is a project initiated by the German and French governments and launched in 2020, during the German presidency of the EU. Today it is a European non-profit association with 377 members. Its members include leading European companies and the main digital service users and providers. The association is open to participation by non-European companies, and indeed includes major US and Chinese technology companies. However, only companies with headquarters in Europe can be on the association's board. In principle, the project is supported by several European governments. Its stated goal is to provide a transparent and secure federated infrastructure to ensure that cloud providers' data and services are governed by common European rules. It was initially presented as a key project for achieving European digital sovereignty in cloud computing. After extensive and difficult internal discussions, it settled into being a project meant to provide a voluntary **technical and regulatory certification infrastructure** on cloud services and data processing. It is likely to become operational in conjunction with the approval of the EUCS.

IPCEI-CIS[ix]

is an Important Project of Common European Interest (IPCEI) on the next generation of edge-cloud infrastructure and services, promoted by the governments of France, Germany, Hungary, Italy, the Netherlands, Poland, and Spain. It will fund the research, development and first industrial deployment of an **open-source middleware platform** and a **common reference architecture** for cloud and edge infrastructure and services. It comprises 19 projects in data processing technologies that cover the entire cloud edge continuum , from basic infrastructural layers of software to sector-specific applications. The projects have been proposed by 19 companies (see Figure 7) which should add €1.4 billion in private investments to the €1.2 billion funded by governments. It has been called "the largest open-source project in EU history",[x] because of the central role of open-source software. Its results will in fact be released under permissive and nonrestrictive open-source software licenses, while project-sponsoring companies will have to actively engage and contribute to the development of open-source communities. This centrality of FOSS has been sought by the EU Commission itself to reduce the distorting effects of state aid on competition and to maximise the spillover effects of investment. It can be seen as a precedent for future IPCEIs and will provide an impetus for European industry involvement in the FOSS production model.

The European Alliance for Industrial Data, Edge and Cloud[xi]

was created in 2021 by the EC. It is formed by main European industry players, representatives of member states and experts. It is exclusively open to businesses that have a legal representative established in the European Union. It operates through working groups and defines an edge-cloud strategic industrial **roadmap for areas of joint investment**, development and deployment. It also advises the Commission on common European standards and requirements for the public procurement for cloud services and data processing services to ensure a harmonised European approach and corresponding practices in public sector bodies across member-states.

Simpl[xii]

was initiated in 2023, funded by the EC through the DIGITAL Europe Work Programme. It aims at providing a **prototype middleware** for cloud-to-edge federations of common European **data spaces**, guaranteeing self-determination in data sharing (sovereignty), confidentiality, transparency, security, and fair competition.

The open European software-defined vehicle platform[xiii]

is a project conceived by the EC in 2023 in agreement with German, French and Italian car manufacturers' associations, with the support of McKinsey & Company. It is a concept paper currently proposed under the EU Commission Key Digital Technologies Joint Undertaking. It aims at promoting collaboration among EU automakers on "non-differentiating **pre-competitive software** developments" and creating an **open reference architecture** and standardised and non-differentiating software elements, such as interfaces and middleware. It is meant to follow an open-source strategy and maintain close links with the EU initiative on a RISC-V High Performance Automotive platform.

MyHealth@EU[xiv]

is a planned EU Commission-led **platform and pilot project** to develop a decentralised pan-European infrastructure for the governance and secondary use of health data. It aims at implementing the health data space regulation. It should be based on cross-border interoperability requirements, common technical standards, and mandatory certification schemes. Around such a platform, an ecosystem should form comprised of common rules, standards, infrastructures. The platform should ensure citizens' rights regarding their own data, transparency, security, safety and privacy, while at the same time facilitating the permitted uses of health records and the authorised secondary use of data.

Alliance for Internet of Things Innovation (AIOTI)

was initiated by the European Commission in 2015 and became an association in 2016. Its members are IoT industrial players, European research centres and universities, associations and public bodies. Its aim is to promote collaboration in IoT and edge computing research and innovation, standardisation, and ecosystem building.

The European Open Science Cloud (EOSC)

is a European Commission initiative started in 2015, aiming at developing a federated infrastructure for services promoting open- science practices. In the initial phase of implementation (2018-2020), the European Commission invested around €250 million in prototype components. It is steered by a tripartite governance involving the EU represented by the European Commission, the participating countries represented in the EOSC Steering Board, and the research community represented by the EOSC Association.

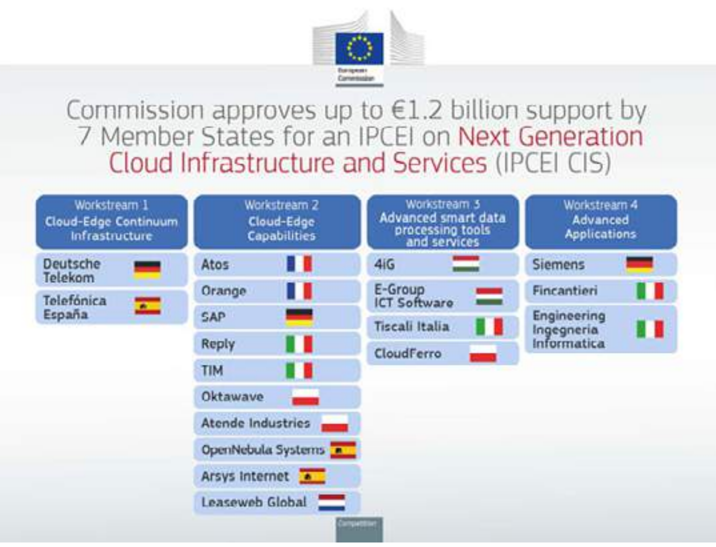


Figure 7 — IPCEI-CIS participants

4.0

THE KEY TEST: PUBLIC ADMINISTRATION CLOUD MIGRATION

The use of IPCEIs is one of many signs of the accelerated change of context in which European digital policy is developing: a world in which the neoliberal Washington Consensus is rapidly waning and industrial policy is becoming an imperative. This means that the EU is being forced to reorganise the way it functions and its policies. In this sense, digital policy is going to be a test case for the EU's new industrial policy and credibility (EPSC, 2019; Terzi & al., 2022).[xv] Suffice to say that 20% of the Recovery and Resilience Facility (RRF) - that is €160 billion - has been dedicated to digital investments. This could be a unique opportunity to fuel the EU's strategic goals. However, the use being made of these resources is also a sign of the risks of a new EU fiasco.

The test case for the EU's digital policy and aspirations of autonomy is undoubtedly going to be the public administration (PA)'s migration to the cloud. This is true for at least two reasons. The first is that in order to secure the most critical data of both citizens and the public administration, the main European countries have each developed their own doctrine based on the need to guarantee such data **immunity** from access by non-European authorities.

This is especially related to the **US Cloud Act**,[xvi] approved in that country in 2016, which obliges US tech companies to allow federal authorities access when they require it , even when these data are stored in third countries. The obligation to preserve the security of this data means that public procurement for critical public administration services could become a protected market for European cloud providers - and provide a critical mass for implementing a new standard architecture for cloud infrastructure. The second reason is that the migration of the public administration to the cloud is, so to speak, **the mother of all investment expenses** in the cloud infrastructure of a country and of the EU as a whole. This is, therefore, a unique opportunity, as the Berlin Declaration of the European Council itself stated. Missing this chance could be like missing the boat for the EU's digital sovereignty ambitions.

4.1

THE ITALIAN *POLO STRATEGICO NAZIONALE* AS A FLAWED BEGINNING

However, if we look at Italy, which is the largest beneficiary of the RRF, the picture is quite bleak. Italy is the first large European country that has undertaken a plan for the organic migration of the public administration to the cloud. The plan is called ***Polo Strategico Nazionale*** (PSN)[xvii] and is financed by the EU Recovery and Resilience Facility.[xviii] Looking at the PSN, Italy has classified three levels of data sensitivity and secured the most critical data from direct management by US companies. The plan also takes a multi-cloud approach to reduce dependency on a single technology provider. However, the technologies that will be used are those of the US hyperscalers: specifically, those of Microsoft, Google and Oracle.[xix]

This is going to happen through a system of licenses that will be transferred to the PSN, which is managed by a consortium of Italian companies with a strong participation of the public sector. On closer inspection, therefore, most of the resources that will be invested will end up **strengthening** Italy's **technological dependence** and an important proportion of them will be directly feeding the turnover of the main US cloud computing providers.

This risk is actually generalised in Europe. European providers are very small and not coalesced around common technological solutions. And it does not seem that a European offer suitable for accelerating the migration of the public administration is ready. Yet this same acceleration – for both the public and private sector - is a goal that was set by the Commission in the *2030 Digital Compass: The European Way for the Digital Decade*.

In the case of Italy, the plan was further accelerated by the tight deadline imposed by the use of RRF resources. Yet this seems like self-defeating. In current conditions, in fact, the result of this acceleration will be to aggravate Europe's technological and economic dependence in the digital sphere.[xx]

4.2

THE PROBLEMS POSED BY EXISTING GOVERNANCE

Still looking at the Italian PSN, another remarkable aspect can be observed: the evident **lack of coordination** between European governments. The Italian plan does not refer to European strategies or to the search for common solutions, not even in terms of standards and interoperability.

One of the reasons behind this lack of coordination is that the governance system of strategic digital decisions has not changed, not even at the more infrastructural level. On the contrary, the digital sphere is currently one of the areas in which the subsidiarity principle has been applied the most.

The result is a great **decentralisation of decision-making** and a huge **fragmentation of public digital systems**. In Italy alone, for example, there were an estimated 1,252 data centres in 2020.[xxi]

This approach has not changed despite the fact that it is anachronistic in the face of the large-scale design coordination and governance required for the next generation of digital infrastructure and the scale of investment required from the public administration. Under these conditions, even if there were the political will and ability to converge on common solutions across European governments, it would not be easy to pursue a coherent and effective digital policy line.

For example, even simply at the Italian level, adherence to the PSN model is voluntary, and each administration will have to decide whether to migrate its systems and data to the more centralised hubs that PSN is building. All the indications are that it will not be easy to convince the various local and sectoral administrations to join the PSN model, despite the resources that will be freed up. This is not least true given that regional public digital agencies and autonomous national administrations have already made investments to support their cloud migration plans, and PSN has not coordinated with them.

4.3

THE *CLOUD DE CONFIANCE*: A PROTECTED AREA FOR FEEDING FRENCH CHAMPIONS

The French government has gradually clarified its cloud strategy for public administration. Initially, the strategy was concerned with securing data from interference by non-European authorities, especially US ones, albeit without excluding the possibility of using the technologies of US hyperscalers through the transfer of licenses to companies under French law.[xxii] Italy followed this "French model" when it accelerated its public-administration migration plan in 2021, in order to respect the strict EU-imposed timeline for the use of RRF funds. In France, however, this solution has more recently been reconsidered and deemed inadmissible.[xxiii]

The given explanation for this is technical in nature. The periodic and constant updates to which the software systems would be subject would require opening access to these systems to the parent company that owns the technology. Beyond that, the French government - and the French EU Commissioner Thierry Breton - are the main proponents of a strong interpretation of the European digital sovereignty and promoters of an industrial policy that supports the formation of **European** (or rather "French") **champions** in cloud computing.[xxiv]

In France, industrial strategy is based on the creation of a Sector Strategic Committee (CSF) open only to French cloud players, meant to coordinate industrial players and French government; and in the parallel promotion of the IPCEI on cloud-edge computing at a European level, which frees up the possibility of public-aided investments in the next generation of cloud technology. But all in all, the main tool envisaged to achieve this goal is regulation.[xxv]

In addition to requesting the inclusion of the cloud among the Core Platform services of the Digital Market Act, subject to specific anti-monopoly legislation, the French National Agency for the Security of Information Systems (ANSSI) has approved a certification system for the security of Cloud services (SecNumCloud),[xxvi] which the French government is now exporting to European agency ENISA (see Box 4). Accordingly, the strictest EUCS certifications which will be released by ENISA should guarantee the **exclusion of non-national or non-European providers** from the public procurement market for the management of the most critical public-administration services and data.

4.4

THE GERMAN MODEL: CONSISTENT, BUT POORLY FUNDED AND UNCOORDINATED

The German strategy for the cloud of public administrations - the Trusted Cloud - is the one that most consistently follows the lines declared in the Berlin Declaration (IT-Planungsrat, 2022). This should be no surprise. In fact, it was during that rotating German presidency of the EU that the main axes for the innovation of European digital policy were outlined for the first time, and the watchword of European digital sovereignty was taken up.

During that same semester, Gaia-X was launched, initially as a partnership between France and Germany, although the concept had actually been incubated in public-private working groups within the German Ministry of Economics. In this sense, while politically the authorship of the EU's digital turn largely owes to Angela Merkel's government, at the technological level the concept is primarily a product of German engineering culture. It is therefore unsurprising that the German plan for the migration of public administrations to the cloud is a coherent and detailed development of the guidelines presented in the 2020 Berlin Declaration.

The German plan involves the definition of a **layer of standardised components, modules and interfaces that must guarantee interoperability** between administrations, "vendor-independence" and the ease of switching providers or technology. The standards are defined by a public-led body in which private industry and experts also participate . Standards are in principle mandatory and enter into the merits of architectural and technological choices, favouring open-source solutions and specifically the architecture supported by Kubernetes. This is an open-source software for the orchestration and management of container applications, developed by the Cloud Native Computing Foundation,[xxvii] and which has become a standard architecture adopted by all the main cloud providers in the world.

The German plan is also compromised with the adoption of the solutions, standards and interfaces developed by Gaia-X for the creation of a European federated data infrastructure, that should guarantee data sovereignty, transparency and interoperability. In parallel, the German plan supports the Sovereign cloud stack (SCS): a project that aims to develop a federatable and fully open software stack for cloud service providers. The development work involves the use of already-tested standard modular software components.

At the same time, the development of additional solutions funded by the public administration should systematically promote open-source solutions and take place on a platform owned by the government (Open CoDE). It is hoped that standardised solutions will create a robust market and increase the negotiating power of public administrations to obtain more cost-effective bids.

The architecture is federated and includes a multiplicity of data centres operated by the federal government, individual states and municipalities, although a coordination entity is envisaged, which will have the responsibility of enforcing standards as well as managing the development platform and the portal for common services. So far, the German government has not yet issued clear instructions on the possible involvement of foreign hyperscalers. But the management of public services and data is divided into three areas, like the Italian plan, with strengthened guarantees: the external, the internal and the reinforced internal. The plan is still in the pilot testing phase.

The German government has also created a Sovereign Fund to support open-source critical components and infrastructure. As a whole, this is an organic and coherent plan. Its main limitations seem to be the slowness of implementation, the scarcity of resources allocated to its development, and the lack of any coordination with other European governments. The latter seems to be the major weakness.

Without the convergence of a critical mass around common architectures and developmental paths, the rollout of stand-alone solutions seems risky and doomed to repeat mistakes already seen in past adoptions of open- source solutions by public administrations, which have not proven vital and sustainable in the long run (Berlinguer, 2020b).

4.5

THE EUROPEAN PLAN FOR PUBLIC ADMINISTRATION MIGRATION, IF IT EXISTED

While Italy limited itself to guaranteeing national management of the most sensitive data, the plans of France and Germany combined could outline the contours of a possible European strategy for the migration of public administration towards the cloud, which is at the same time technological, regulatory and industrial.

If we entered into an exercise in abstraction and outlined this strategy in just a few words, as if it existed already, then these would be its main characteristics.

Technologically, its core infrastructural components would realise the principles set out in the Berlin declaration: open-source software, common standardisation, modularity, and interoperability. This choice of technology would be based on **consolidating common building blocks**, and **leveraging** the more **mature open-source** components that already form the backbone of cloud infrastructures. It would furthermore proceed by sharing efforts and results - through common standardisation and publicly funded FOSS developments – so as to progressively piece together an organic and complete stack of common open-source technologies, at least for the most basic infrastructural levels and for the most common public-administration services.

The regulatory arm would reinforce this strategy by making these principles, standards, technological specifications, and interoperability rules **mandatory** for public administrations and for critical service infrastructures. This could perhaps involve excluding non-European providers from these markets, at least in the most sensitive services, either for security reasons or because of the need to protect EU citizens, business and governments' most sensitive data from extraterritorial surveillance activities by foreign authorities, and ensure full compliance with the stricter EU regulations on citizens' privacy.

These two conditions combined would create a space for nurturing a European cloud industry, first by encouraging European providers to coalesce around these common technological building blocks, architectures and specifications, and secondly by creating a **protected market** to grow European cloud providers. This convergence could foster the formation of "European champions" as in the French version. Or, in a less centralised model, it could promote the formation of **federations or consortia** of software component "**aggregators**", around these common infrastructural building blocks.

These consortia could form an important green shoot for an autonomous European cloud industry and sustain the development and maintenance of European common standards. Moreover, the formation of this ecosystem of providers and users would help to tackle some of the weaknesses that FOSS components sometimes display, creating the conditions for introducing innovative arrangements aimed at reinforcing the maintenance, development, and compatibility of these same infrastructural components (see Box 9). Furthermore, around these infrastructural layers an **ecosystem of services and applications providers** could develop, relatively free from the risk of being trapped in platform vendors' lock-in strategies.

This same pattern can inform (and has been designed to inform) a common European policy for areas of innovative cloud-technology development. Governance in innovation is different and certainly more complex than consolidating existing mature components and solutions through standardisation efforts. The difference resembles the dichotomy between exploration and exploitation (March, 1991), which, in software, is more commonly defined on the basis of the "maturity" or "stabilisation" of certain technological components or packages. Yet also with regard to innovative developments, EU policy relies heavily on standards – at least in theory - and they are definitely an important road. The same principles applied here push toward investing in and promoting open standards and open-source solutions. This is envisioned in the new Edge-Cloud-IoT architecture which is promoted by initiatives like Gaia-X, the IPCEI-CIS, the European Alliance for Industrial Data, Edge and Cloud, and it is applied in tentative experimental implementations such as Simpl or the Open European software-defined vehicle platform (See Box 8).

It seems that the main difficulties here concern the possibility of aggregating a critical mass of adopters, users and developers around the chosen technology options, instead of proceeding in isolation, as has been done too many times in public-sector-supported open-source projects. Another challenge is how to calibrate the adoption of standards with strategies that minimise the risk of being locked into a single trajectory and that instead maintain flexibility and resilience, including by encouraging exploration, redundancy and the pluralism of paths (Benkler, 2016), for example, combining standards with modularity and with design efforts for compatibility and interoperability.

A strategy of this kind, moreover, would mimic and attempt to exploit the practice of **competing by proposing open-source solutions**, a practice which is now widespread between large technological companies in their "standard wars". This is aimed at aggregating a critical mass of developers and enterprises around their technological platforms in order to accelerate adoption and innovation. AI itself - probably the most impactful of the last generation of digital technologies - could be another terrain on which to test a policy of this kind. As in any frontier of digital innovation, in fact, a fierce competition is growing between tech giants, and open-source solutions are already being used to catch up and reverse initial disadvantages, accelerate adoption and innovation. The EU could accelerate this evolution.[xxviii]

However, in both cases - the consolidation through standards of more mature technology layers and the push for adoption of open-source solutions and open standards in the development of innovative technologies - the most challenging aspect is probably the creation of innovative governance models. These could probably take on some of the characteristics of the latest generation of FOSS foundations and the forums they organise. These are the organisations currently driving the development of the most advanced and complex FOSS initiatives, including the most important cloud technologies. The Cloud Native Computing Foundation and the Open Infrastructure Foundation are examples of this. However, the presence of state actors and public goals would change and reformulate the functioning of these spaces. Figuring out how to do this is a task that is still waiting to be outlined and addressed. (See also section 5.3).

Free and Open-Source Software security: a societal problem

BOX 9

There have been several episodes of suddenly discovered vulnerabilities in very popular FOSS programmes, which have caused waves of global panic. This is because sometimes these FOSS components are used by millions of organisations, including the largest tech firms, such as Google or Amazon, or by the most important governments, for example, US government departments or European Union directorates. These incidents have helped bring to light the complexity of the "dependencies" that characterise complex digital systems today, and the lack of awareness on the part of even the largest and most sophisticated organisations about the nature of these technological dependencies and of the forces on which their maintenance, updating and security depend.

For example, the Heartbleed case[xxix] showed how a critical application in security systems used by millions of organisations depended on just a handful of developers, who maintained it almost exclusively on a voluntary basis, with virtually no resources. In another famous case - NPM "colors" and "faker"[xxx] - it was one of the developers who deliberately introduced errors into some libraries, downloaded millions of times each week and on the operation of which thousands of other programmes depend.

In that case, this action was a form of protest and retaliation against mega-corporations and commercial consumers of open-source projects who extensively rely on cost-free and community-powered software but do not, according to the developer, give back to the community. Finally, another recent headline-grabbing case was the one that hit Log4j, a ubiquitous, open-source Apache logging framework library that put a very large portion of Internet-connected digital systems at risk,[xxxi] in this case triggering more robust governmental initiatives.[xxxii]

A recent report gives an Idea of the extent of the systemic and societal problem not addressed by existing governance in the FOSS ecosystem. According to this survey, 96% of the software that was scanned contained open source, and, on average, 76% of the systems were made of open-source components. At the same time, 84% of the scanned software contained at least one vulnerability and 48% of the programmes contained high-risk vulnerabilities (Synopsis, 2023).

Overall, these incidents have led to the institution of a number of "ecosystem-wide" initiatives aimed at better securing FOSS digital "infrastructure." In several cases, governments themselves have promoted these initiatives. Among these, the main ones have been the Core Infrastructure Initiative,[xxxiii] later evolving into the **Open Source Security Foundation,**[xxxiv] both organised under the auspices of the Linux Foundation, both funded by the tech industry, and in the latter case promoted under the impetus of the US government.

In Europe, the EU Commission activated for some time the **FOSSA** bug bounty programme,[xxxv] while the German government recently established the **Sovereign Tech Fund**[xxxvi] to fund and ensure FOSS critical infrastructure. Legislation is also being drafted to strengthen the security of digital systems and FOSS specifically, for example in the EU with the **Cyber Resilience Act** (CRA)[xxxvii] and in the USA with the **Securing Open Source Software** Act (SOSSA).[xxxviii]

The problem is far from solved, however. It remains very challenging, because of the enormous amount of programmes that need to be secured; the complexity of these systems and of the dependencies that constitute them; the decentralised and uneven nature of the initiatives that generate, maintain and update these systems; and the difficulty of finding effective and fair mechanisms for distributing the burdens and benefits generated by these systems' creation, maintenance, use, and securing.

The draft European CRA, for example, is drawing sharp criticism from many in the FOSS ecosystem. CRA aims to force commercial software distributors to take responsibility for programme security by making good security practices mandatory, as also happens in other sectors. Prominent voices in the FOSS world, however, have accused it of altering the "social contract" that underlies the entire open-source ecosystem.

FOSS, in fact, is provided for free, can be modified and further distributed for free, but is ostentatiously released and disseminated under licenses that disclaim any responsibility or warranty for the authors, contributors or distributors of the software. The clash around the CRA highlights how FOSS has become a pillar of digital society, and thus its security is becoming a concern for governments. However, according to these critical voices, CRA fails to adequately define, organise and distribute burdens, incentives and support among ecosystem players, thus risking overburdening FOSS developers and small businesses with compliance work and failing to streamline a proper certification process that adheres to the complexity of FOSS production characteristics (Phipps, 2023).[xxxix]

According to some (for example, Milinkovich, 2023), CRA could even incentivise the introduction into FOSS licenses of clauses that cut off Europe from the free use of FOSS programmes, so that they can be shielded from the risks of being brought to task for unjustified and unwanted responsibilities.

On the other hand, the proposed SOSSA bill in the United States follows a light-touch regulatory approach. It envisages a new office in the federal government responsible for mapping and monitoring infrastructure risks in the FOSS programmes on which government and critical infrastructure depend, while maintaining a voluntary framework based on private industry incentives to promote public-private partnerships to improve FOSS security.

However, SOSSA is subject to opposite critiques, according to which it fails to introduce a clear system of liability and therefore of incentives that ensures that security problems are routinely researched, identified and solved. In so doing, it fails to intervene in the basic failure that the FOSS ecosystem is exhibiting, namely, society's insufficient investment in the security of open- source software, which contrasts with the systemic reliance upon it.

Ultimately, addressing the security of FOSS involves addressing the unresolved problems that run through this innovative production model. One of these is the **unequal distribution of burdens and benefits that FOSS - as an open-access common good - generates**, which has serious side-effects, for example, in the habitual lack of time, of incentives and of sustainability that plagues those who maintain of these systems. Another is the **fragmentation and insufficiency of effective mechanisms to coordinate** a process of innovation, production or securing that is itself highly decentralised and dynamic. In developer jargon, we might refer to this as the lack of a "single point of truth." Addressing these unresolved issues suggests a space for innovative public policies.

This is a topic to which we will return in Part III.

4.6

EU STRATEGY: MISSING CLARITY, CONSISTENCY AND DETERMINATION

Still, as we said, all this was just an exercise in abstraction. In reality, things have taken a different course. Overall, EU governments failed to exploit the opportunity of using the RRF funds to push for a coherent and coordinated strategy in the migration of the public administration to the cloud. More generally, it is easy to point out limitations and contradictions of these public-administration migration plans. We could cite the slow pace of implementation, which clashes with the acceleration of cloud adoption aimed for in the EU's Digital Decade plan; the scarcity of resources allocated to these plans; and, most importantly, the lack of consistency, coordination and alignment of national plans.

And this picture, made up of a lack of determination, coherence and clarity, would be magnified yet further if we widened our perspective to include all EU member states. Behind this situation, some structural weaknesses can be easily identified.

In the first place there are uncertainties, hesitations and divisions on the **nature of EU strategic autonomy** in the digital sphere, especially in relation to the USA (but hesitations, oscillations and inconsistency exist on 5G and Chinese providers too). This is a source of ambiguities in each step and in each direction. The stories of the "sovereign clauses" of the EUCS (see Box 6) - under discussion for over three years - or of the new agreement on the transfer of personal data of European citizens to the USA (see Box 3), are illustrative, in this sense. And Russia's invasion of Ukraine has clearly further weakened the EU's aspiration for autonomy. The most obvious consequence of this lack of clarity, determination and consistency is that it does not allow the definition of any kind of sustained, convergent and congruent investment to fuel a coherent European cloud strategy.

The second underlying reason is the **absence of a significant European cloud industry** and, more generally, a strong autonomous digital industry (see Figure 4). Like governments, the main industries in the European market have settled into a position of users and consumers of digital technologies. This vacuum of strong European economic actors in the digital sphere probably has facilitated the possibility of regulatory intervention, as resistance from domestic lobbies is weaker. But it denotes an accumulated structural weakness that would require much effort and innovative approaches to be breached.

And, though some elements of innovation have been outlined, a common and cohesive political will does not have emerged, and to take form it would have to overcome no few resistances. After all, any industrial policy can easily lead, at least in the beginning, to inefficient and ineffective results, and especially to unequal economic advantages and disadvantages. This may in turn ignite conflicts between different governments, countries, and economic interests, for instance reinforcing the hostility of smaller countries and economic sectors that are users and not providers of cloud technologies, and that do not see much benefit in trying to build a European cloud industry through subsidies or protectionism.

Finally, there is a structural **inadequate governance** for the digital transition in EU public administrations. The extremely decentralised system of competencies in the digital sphere has historically been a major source of weakness and resource wastage in European countries and in EU public procurement. It has made it easy to trap European public administrations in costly lock-in strategies (European Commission, 2013; Berlinguer, 2020b).

It has frustrated multiple public-administration harmonisation plans and collaboration programmes, as with the substantial failure of the EU's ISA and ISA2 programmes (Renda & al., 2021). This lack of coordination is an even more glaring problem in view of the infrastructural nature of cloud computing systems. There is an obvious need for a **more unified agency** (Florio, 2020), if only simply to reduce costs, avoid dispersion of resources, provide competent leadership, and simplify migration plans. This coordination is an objective that a new legislative proposal - the Interoperable Europe Act (see box 10) - aims to bring closer, at least giving legitimacy to a more shared governance of public-administration digital systems. But frankly, it is hard not to see this as a classic case of "too little too late."

Interoperable Europe

BOX 10

The Interoperable Europe Act (IEA) is the name of a regulation proposed in 2022 to improve cooperation and interoperability among national public administrations within the EU on data exchanges and IT solutions. It follows the disappointing results of the European Interoperability Framework (EIF) - a set of recommendations for administrations within the EU - initially introduced in 2004 and subsequently updated and carried forward by three different programmes called: the IDABC, ISA1 and ISA2 (Renda & al., 2021).

All these initiatives were based entirely on a voluntary approach, hence the idea of introducing a more stringent instrument with the Interoperable Europe Act. In reality, the only additional mandatory provision that the IEA would introduce is limited to requiring an assessment of the impact of any choice of IT systems on pan-European interoperability, and its stated aspiration does not go beyond the creation of a "network of sovereign digital public administrations." The main goals of a European interoperability framework are to improve cross-border interoperability between administrations and public services, to share and reuse solutions, often based on open source, to accelerate the digital transformation of the European public sector, and to save costs for public administrations, businesses and citizens dealing with public administrations. A further step envisaged by the IEA is the establishment of a common governance system through the creation of the Interoperable Europe Board. However, it is difficult to imagine a decisive breakthrough coming from this body, composed of representatives from the EU member States, the Commission, the Committee of the Regions and the European Economic and Social Committee.

3

A MATRIX FOR RETHINKING PUBLIC GOVERNANCE

⇢ 5.0

AN UNFINISHED WORK OF INNOVATION

To what extent is there really a political will and unity in favour of European digital autonomy, among the EU's governments? Will the EU countries find a way to overcome internal divisions and converge on common and implemented - as opposed to simply declared - solutions on the regulatory, technological and productive terrain in cloud computing? To what extent is the EU able to implement innovative, effective and unifying industrial policies? These are some of the many questions that fuel doubts about the outcomes of European policies on cloud computing.

Amid these doubts and uncertainties, the EU has nevertheless begun to deal with an important issue: the construction of new instruments for the political governance of the new generation of digital infrastructures. There are numerous aspects of the EU's cloud computing plan that would deserve critical investigation and a better understanding of their challenges, innovations, limitations or implications.

Figure 8


Berlin Declaration
on
Digital Society and
Value-Based Digital Government

at the ministerial meeting during the
German Presidency of the Council of the European Union
on 8 December 2020

(5) Digital sovereignty and interoperability

Digital sovereignty is key in ensuring the ability of citizens and public administrations to make decisions and act in a self-determined manner in the digital world. We must ensure that all underlying digital components of ICT solutions (hardware, software, and services) meet European requirements. We must create the right conditions for Europe to develop and deploy our own key digital capacities, including the deployment of secure cloud infrastructure and interoperable services that fully comply with European legal provisions and ethical values. Common standards, modular architectures and the use of Open-Source Software (OSS) in the public sector are facilitators for deploying and developing strategic digital tools and capacities. We must ensure the availability of diverse and high-performing digital solutions to guarantee freedom of choice and the ability to change IT modules when necessary. Software, data and tools generated by the public sector should be reusable and openly accessible as long as this is compliant with fundamental rights. As explained in the European data strategy, a strengthened interoperability framework, as well as suitable regulatory frameworks are key in helping Europe benefit from the economic value of data, thus creating a single market for data that will ensure Europe's global competitiveness and data sovereignty.

In this last part, we will make some effort in this direction by focusing on one single aspect of the EU strategy, which is perhaps the most original: the principles of technology design and development identified in the EU cloud strategy.

In the following, we will frame these principles as rooted in a matrix that has grown and evolved organically in the development of digital technology and explore the motivations that have brought these principles to the fore, indeed so much so that they were enshrined in a solemn political declaration by the European Council in 2020. We will then try to answer some questions. What are the most notable features of these principles? What can their adoption by EU policy teach us in terms of innovations which are underway in the governance of large digital technological systems? The following analysis will allow us to highlight areas in which we should expect public policy innovations, but which do not seem to have been sufficiently thematised in EU policy thus far, and which could play a critical role in renewed current attempts to develop policy governance regarding large technology systems and digital infrastructure, even beyond the case of the EU.

⇢ 5.1

AN INNOVATIVE MATRIX OF PRINCIPLES OF TECHNOLOGICAL DEVELOPMENT

The technology design principles to which we refer were first presented in the aforementioned Berlin Declaration: which is to say, the European Council Declaration on Digital Society and Values-Based Digital Government in November 2020 (European Council, 2020). They are presented in the chapter 5 of the declaration, entitled: "Digital sovereignty and interoperability" which succinctly summarises the European strategy in the digital field and in cloud infrastructures (see Figure 8). There, we find a reference to digital sovereignty, in its most peculiar sense, the one that emphasises the preservation of the autonomy of choice and action in the digital world. Reference is made to the role of the public sector as a lever to support a deployment of these systems. There is also an explicit reference to data sovereignty, as the backbone of the EU's competitive and economic strategy. But above all - and this is the most unusual aspect in a political declaration - we find a set of principles with which European digital infrastructures and systems in the public sector should comply: **interoperability**, **common standards**, **modular architectures** and **open-source software**. All these are principles of design and development of technological architectures and systems (See Box 8).

The Matrix: four principles for EU cloud sovereignty

BOX 11

The Berlin Declaration sets out four principles as benchmarks for building "sovereign" cloud infrastructures. These principles actively applied in many of the initiatives, legislative and otherwise, that the EU has undertaken in recent years with the aim of regaining spaces of autonomy, control and self-determination in digital systems – or rather, dismantling the monopolistic position of digital gatekeepers (see Box 5 and Box 8).

The governance of these design and technology development principles, and their intertwining, are already very important in the current constitution of digital systems. They are principles that help manage the increasing complexity of these systems, but they also influence the freedoms and constraints of the different actors operating within these systems, the possibilities for innovation, and the economic models that are established at the different levels and layers of today's digital ecosystems (Berlinguer, 2021).

EU interest in these principles indicates that they are becoming a new focus for public authorities and public policy. An important question in the near future will be: how will the intervention of state actors influence the dynamics and governance of these principles?

Interoperability

The term "interoperability" refers to the ability of a system or product to work together with other systems or products (Wegner, 1996). In information technology, it refers to the possibility of exchanging information between systems. With the increasing complexity and integration of digital systems, one of the most important challenges facing large-scale systems is the interoperability of their component systems (Rezaei & al., 2014). (see Box 2)

The concept of interoperability has progressively expanded its application. The EU has for the last two decades faced struggles in its attempts to foster interoperability among European public administrations in member states, with the objective of facilitating communication, coordination, simplification, resource saving and the creation of a common market for public administration services. In response, it has moved to classify four types of interoperability: the syntactical, technical, semantic and organisational.

A smooth internal technological interoperability and - conversely – an external proprietary, unilaterally modifiable interoperability, represent a key tool and competitive advantage used by large platform companies to achieve high levels of technological integration in their systems, while at the same time controlling and selectively opening their platforms to services and applications offered by third parties (Sharma, 2019).

On the opposite side, more recently interoperability has attracted a great deal of interest in anti-trust debates. Interoperability is seen as a potential tool to combat lock-in strategies and monopolistic practices in digital platforms and digital markets. It is seen as an alternative to more drastic interventions, such as breaking up dominant monopolistic companies (Sharma, 2019; Kades & Morton, 2020). Interoperability is a mandatory requirement in telecommunications, for example, and in this sector it - together with other norms - allows customers of different telephone companies to communicate with each other and to change telephone companies, without technological obstacles.

On paper, the EU has long since introduced regulations that require interoperability rules in digital services. The GDPR, approved in 2016, already provides for the right to personal data portability and switching between different digital service companies; and this was reinforced by the regulation on the free flow of non-personal data (2018).

Following those provisions, a laborious process of self-regulation led in 2020 to the definition of SWIPO (Switching Cloud Providers and Porting Data)[xl] voluntary codes of conduct for cloud-service providers. However, more recently the Digital Market Act has introduced more stringent and mandatory rules of interoperability for the "gatekeepers" in "core platforms services" (see Box 5), with very onerous fines in case of non-compliance. And the proposed Data Act contemplates the introduction of a binding obligation for cloud-service providers to offer data and application portability, giving the EU Commission the power to introduce interoperability specifications and standards.

Standards

If the notion of interoperability can be applied to a broad range of integrative efforts, the term "standard" has an even wider scope (Edwards, 2004). Technical standards represent an important family of standards, but not the only one. In general, this term refers to something established as a rule, a model, or a measure, by authority, custom, or general consent. Kindleberger (1983) distinguishes two classes of standards in an economic perspective: those that create economies of scale and those that lower transaction costs.

Depending on the procedure through which they are established, standards can be classified as: *de facto*, *de jure* or developed by recognised standard organisations. In the last decades, in ICT, governments and recognised international standard developing organisations (SDO) have been increasingly pushed aside in favour of *de facto* standards, and standards have often become the terrain of "standard wars" (Varian & Shapiro, 1998) in the market (according to the rule "the winner takes all").

Otherwise, they have been pursued through private consortia or by a plethora of new competing standard-setting organisations (SSO). In software, however, Free and Open-Source Software has gradually emerged as an outsider and unexpected protagonist in the *de facto* global standardisation scene (Burson, 2018; Knut & al., 2019; Berlinguer, 2021). More recently, governments are showing a growing interest in retaking a role in standard-setting, sometimes allying with FOSS in this effort. Indeed, China's ambitious standards strategy in emerging technologies - revealed in the China Standards 2035 programme, published in 2018 - was one of the alarm bells that most contributed to the turning point in the USA's and EU's relations with China (Liu & Cargill, 2017; Seaman, 2020).

The EU has long identified standards as a crucial lever of its technological and industrial policy, and from 2016 began to develop a standards strategy, both for improving internal homogeneity and in the attempt to influence the international competition in emerging new technologies (European Commission, 2016).

More recently the EU has taken on a more proactive orientation. The most recent legislation, in several areas related to cloud computing, has granted the Commission the power to choose and adopt technical standards in emerging technologies.

Modularity

The concept of modularity has since the 1980s increasingly been adopted in many disciplines: technological and industrial design, organisational studies, biological sciences, ecology, psychology and cognitive sciences. In general terms, modularity refers to systems made of components - modules - which can be separated and recombined. It has its conceptual opposite in tightly integrated systems.

It is an architectural strategy generally associated with the need to reduce complexity, maintain flexibility, and reinforce systems' resilience (Simon, 1962; Ethiraj & Levinthal, 2004; Garud & al. 2009). It also simplifies the organisation, management and coordination of the social division of labour (Baldwin & Clark, 2000; Langlois, 2002).

In modular systems, each component can be developed or modified autonomously and be easily integrated in larger systems, thorough interfaces, standards or architectural design rules. Modularity has become a typical characteristic of large software systems and it is a strategy largely utilised in software development. Among the advantages attributed to software modularity are the fact that it simplifies a decentralised division of labour and innovation, reduces cognitive complexity, facilitates adaptability, evolvability, and provides a simple way to assemble re-combinable varieties and customised solutions (Manovich, 2005; Ethiraj & Levinthal, 2004).

Open-Source Software

(Free and) open-source software – OSS, or FOSS - is software developed and released on the base of licenses that allow anyone to freely use, copy, study, change and redistribute it. Its opposite is proprietary software, which applies restrictive copyright licensing, normally charges for its use, and keeps the source code a secret from users or clients (on FOSS trajectory see also box 10 and section 5.4). FOSS has had a long trajectory and a surprising evolution. Its unconventional way of organising the production of software in fact took its first steps at the margins of industry, within informal communities of autonomous developers. Yet, today tens of thousands of companies participate in the FOSS ecosystem in different ways and it is estimated that between 70% and 90% of existing software systems are made of open-source components (Synopsis, 2023).

FOSS is centre-stage on all the main frontiers of digital innovation, from cloud computing, to IoT, AI, 5G, DLT, and even quantum computing. In certain cases, open-source solutions have become an arena for convergence, standardisation and industry-wide forms of collaboration. Still, in other cases FOSS alternatives have become a central instrument for capitalist competition (Berlinguer, 2018).

Communities are still important in the dynamics of FOSS, and their modes of operation still shape the basic norms that govern the FOSS ecosystem (O'Mahony, 2007). However, the FOSS ecosystem has radically changed. Companies are the main protagonist of FOSS development (Perens, 2005; Berlinguer, 2018; O'Neil & al. 2021).

Some FOSS foundations have grown spectacularly thank to firms' economic support (Krazit, 2020) and Big Tech's influence on FOSS has also expanded, sometimes in problematic ways (O'Neil & al., 2022; Martí, 2022; Pannier, 2023), such as for example with Microsoft's acquisition of GitHub, the main FOSS development platform.

The declaration establishes an explicit relationship between this matrix of principles and the **preservation of conditions of freedom** in cloud computing. Interestingly, we can interpret this freedom in two ways: as maintaining greater flexibility and thus **strengthening the resilience of these technological choices**; and as **reducing the risks of vendor lock-in** and capture for users. Furthermore, these principles are often associated, also in EU documents, with other values such as more competition between alternative solutions, greater democratisation of innovation, transparency, and suitability for decentralised and federated solutions.[xli]

To begin with, there are two points worth making on this statement and the matrix which it highlights. The first is that it helps to bring to the fore the importance of these technological and architectural choices in the governance of digital ecosystems' economic, legal and political characteristics. The second is that this **matrix of principles** to which the EU has decided to entrust the design of cloud architectures is based on trends that have become **predominant** in the development of software systems. These principles are in fact used pervasively in the architecture of present-day digital systems.

Among these principles of technological development, the most remarkable and innovative is without doubt **Free and Open-Source Software** (FOSS). The paramount reason is its ownership regime: FOSS is in fact a **digital commons** (Benkler, 2013). Its most distinctive feature is that it is governed by licenses that allow anyone to access, use, copy, modify, develop and redistribute it. That is, FOSS radically overturns the principle of exclusivity enforced by intellectual property rights (IPR). This basic institutional arrangement has crucial implications for models of governance and ways of appropriating the value of the resource (Benkler, 2013; Berlinguer, 2018). The most obvious of these is that it cannot be directly commercialised.

In spite of this characteristic, FOSS has step by step come to largely dominate software production, i.e. the leading technology and industry of the digital revolution. Arguably, its success has challenged many entrenched beliefs about the need for intellectual property rights to incentivise innovation, and assumptions regarding the failures in public goods provision or in the governance of the commons, in the digital sphere (Arrow, 1962; Hardin, 1968). But before FOSS ecosystems reached this point, their models of governance in have significantly changed.

In fact, to cope with the challenges of its own expansion, FOSS has been a constant source of innovation in governance systems and economic models, which have continuously evolved (Berlinguer, 2023). Indeed, FOSS can be thought as the laboratory of innovations for the new digital paradigm (Perez, 2003; Berlinguer, 2020a). In its initial stage, the main innovations revolved around licensing and the invention of new organisational solutions aimed at facilitating collaboration among dispersed and diversely motivated contributors, in the absence of hierarchical ties or market transactions.

In the subsequent phase, FOSS has been a laboratory for new economic models and new forms of capitalist competition. As we will argue in the section 6.4, FOSS is now entering a third stage of evolution, as, by all evidence, government and public policy are now centring their attention on FOSS (on the evolution of FOSS see also section 5.4 and Box 11).

But FOSS is especially significant also from another point of view. FOSS's trajectory and its success have also deeply **influenced** the evolution of the practices surrounding the other principles of the aforementioned matrix: **modularity**, **interoperability and standardisation**. For example, in software, FOSS is increasingly supplanting traditional standards-development approaches, providing a model for **"open standards"**. This latter model is more informal, agile, and suitable for digital systems, as it is based on continuous and direct implementation (rather than going from specifications to follow a cumbersome path, as is customary for standard development organisations), and at the same time more equitable, accessible, and transparent, as FOSS standards ensure a drastic reduction in barriers to adoption, development, and testing, thanks to the absence of royalties and the freedoms guaranteed by FOSS licenses (Burson, 2018; Blind & al.. 2019; Berlinguer, 2021).

Similarly, FOSS has influenced the approach to interoperability, or the ability of different systems or software components to work together, exchange information and use each other's functionality or data seamlessly. It has fostered this by promoting open protocols and open standards, facilitating adaptability and extensions, and spreading the use of **"open APIs"** (open application-programming interfaces), as opposed to proprietary APIs. It has also facilitated and encouraged the growth of modularity, that is, the design and development of systems made of components that can be easily separated and re-combined.

Indeed, to a large extent, FOSS and modularity have grown in parallel and symbiotically in software production and development, as the partitioning of a project into modular components facilitates the organisation of uncoordinated collaborations and decentralised developments, which fits with the FOSS model, while FOSS licensing has made it easy to reuse modular components — ones which FOSS culture often celebrates as being "permissionless". But maybe the most prominent example of this symbiotic growth is provided by the software development platforms, which have become fundamental infrastructures of the software industry.

All the main platforms have, in fact, incorporated the logic of **"forking"** as the ordinary, default mechanism for facilitating the parallel development of workflows on the same programme. By "forking" they refer to the ability to clone the software and divide its development – initially thought of as a tool of last resort in the hands of FOSS communities to hold project leadership accountable or as a way to resolve internal conflicts over project development.

FOSS, standardisation, modularity, and interoperability have thus come to be increasingly **intertwined** in their **evolution**. Together, these principles can be regarded as a matrix which has become a crucial leverage by which – not simply technological systems development but – **rules and economic models** are being shaped and governed in digital ecosystems. And, although this is neither clearly stated nor directly addressed in EU policy, the most distinctive feature of this matrix is that it is **non-proprietary**. Being a matrix, and being always combined with proprietary layers, however, the configurations to which the possible applications of these principles give rise can be very diverse. The clearest example of this is provided by the parallel growth of widespread FOSS use along with the formation of giant monopolies in the digital sector (Berlinguer, 2018).[xlii]

This apparent paradox also means that the importance of this matrix does not allow any simplistic technological determinism to be deduced and applied from it. Rather, the art of governing and combining the different principles of this matrix is fundamental. Indeed, Big Tech companies have learned to skilfully orchestrate networked activities and ecosystems around their platforms by carefully modulating these principles with closed, proprietary systems. The use of this matrix by the public actor constitutes a decidedly new area of policy experimentation.

5.2

A NEW FOCUS FOR PUBLIC POLICY

But what is behind the success of this matrix of principles, anyway? There is no singular explanation. Furthermore, in the literature they are not treated as a matrix and are instead usually each addressed separately.

However, looking at the diverse literature that has developed around each of these principles, there are two general rationales that are most widely used to justify and explain the adoption of these individual design rules, which moreover largely overlap: that is, to simplify **complexity** management and to reduce communication and **transaction costs** (see for example: Steinmueller, 2003; Baldwin, 2008; Gottschalk, 2009; Benkler, 2013; Blind, 2016).

Therefore, following this common thread, we can interpret this matrix as consisting of a family of solutions that address the daunting complexity and enormous transaction costs implicit in the development of these very large dynamic techno-infrastructures, ***without trying to return to the old solutions – the use of vertical, integrated, and planned forms of hierarchical organisation - that were typical of the Fordist era*** (see Box 12).

Transaction costs and the mutation of the predominant organisational models

BOX 12

Transaction cost theory has attracted strong interest especially with the growth of ICT and the Internet. Transaction costs can be described as the costs and risks that a firm incurs in purchasing a good on the market instead of producing it internally. The economic theory on transaction costs developed organically from the 1970s onward. Its main theorist has been Williamson (1979; 2010). But approaches to transaction cost theory have varied (North & North, 1992). The origin of the concept, however, is older. It is owed to Ronald Coase, and dates back to a famous 1937 article: The Nature of the Firm (Coase, 1937). The article aimed at giving a theoretical explanation of the choice between firm or market ("make or buy", as later would have been said). Historically, however, the background that needed to be explained was the success of the corporate model that emerged with Fordism: large, vertically integrated firms.

What explains the success of this model of organising production with respect to markets? Vertically integrated corporations in fact eliminate the (purchase of goods on the) market through the planning and integration of production processes - sometimes from raw materials to the final product - within an internal hierarchical chain of command (Chandler, 1993). The explanation, in this article, was located in the reduction of transaction costs, although Coase did not use this term. He used the concept of the "costs of the price mechanism".

In the subsequent development of the theory, these costs have been often grouped into three categories: 1) search and information costs; 2) bargaining and decision costs; 3) policing and enforcement costs. But the list of transaction costs has continuously grown as well as the estimate of their weight within the economy as a whole. In general, these are costs different from production costs and not calculated in prices, and they are thus very difficult to estimate. On the opposite side, Coase pointed out - as a limit to the internalisation of processes - the growing costs, inefficiency and misalignment in organisations as their scale grows. Some have subsequently called these latter "internal transaction costs", but this use of the concept is more controversial. The theory of transaction costs has found a broader treatment in the New Institutional School, starting from the 1970s. Within this tradition, markets and hierarchies are represented as two polarities - two ideal-types - around which to study the comparative advantages of the different families of solutions to "coordination" problems (Williamson, 1973). One of the criticisms made to this school is that it is based on an abstract concept of efficiency, as a criterion in choosing the most appropriate form of governance, without taking into account the role that different groups, their interests, and their asymmetries of power have in the prevalent choice of organisational and institutional forms. In any case, the theory brings to light dimensions often completely overlooked by neoclassical economic theories, centred on market mechanisms (and on the implicit assumption of zero transaction costs).

With the ICT and the Internet, many have been prompted to take up the transaction costs theory. The underlying idea is that ICT contributed to radically changing transaction costs and thereby to producing a structural change in the systems organising production. However, in this case, too, the theory took opposite directions. Some have used it to explain the reduction in transaction costs and thus the increase in the market-outsourcing of functions that had previously been internal to companies. Others have used it to explain why the Internet and new communication and information technologies have made internal organisational systems more efficient and easier to monitor and have made it possible for organisations to grow in scale.

The success of transition cost theory is also reflected in its widespread use to explain the organisational advantages of each of the different principles in the matrix which we are analysing. For example, it is employed to explain the advantages of FOSS versus proprietary software, or of modular versus integrated technology design, or of introducing a standard versus a plurality of competing systems, or of interoperable versus closed systems. Although it is difficult to follow a single thread in these arguments and in their use of the concept of transaction costs, the deployment of this concept in explaining the success of these organisational principles surely has helped bring to light a family of organisational solutions which is distinct from the classic market vs hierarchy dichotomy. For example, it has helped to make understandable the advantages of informal, non-hierarchical, and non-proprietary sharing systems, highlighting how they largely eliminate the need for negotiations, contracts, controls and sanctions. Evidently, these systems have their weaknesses, inefficiencies and failures. But, in software they have found fertile ground to grow and spread. And the theory of transition costs has often been used to explain some of their relative advantages compared to market systems. These solutions, however, are also different from the hierarchical models that served in the Fordist era, according to Coase's theory, as a strategy to reduce transaction costs. Therefore, by looking for a unified logic behind these organisational solutions, and their increasing intertwining in software, we can see in them **mechanisms that facilitate decentralised coordination and collaboration** – including often indirect, unplanned, and undeliberate collaboration – **within an open, indeterminate universe of actors, unbounded by hierarchical ties and market relationships**.

Ultimately, their growing importance highlights the need to integrate a third ideal-type form of governance. One of the first to express this necessity, within the New Institutional School, was Powell, who observed the growing importance of business networks as an organisational model on the frontiers of technological innovation and in situations of great uncertainty (Powell, 1990). In this sense, as it happened at its origins, the renewed interest in the transaction cost theory represents a sign that once again **there is a transition in the main organisational forms**. If we look at the matrix from this perspective, FOSS - that is a commons - together with modularity, standards, and interoperability, actually belong to a broader family of phenomena and to a typology of organisational and governance principles which does not fall within the two classic models typified by the neo-institutionalist school, i.e. the market and the hierarchy.

Ostrom - who won the Nobel, in 2009 in association with Williamson, for her studies on the **commons** - called these systems "polycentric", in the sense of characterised by the co-existence of multiple centres of autonomous decision-making (Ostrom, 2010). Commons scholars have ascribed advantages to **polycentric** governance systems, especially in terms of enhanced adaptive capacity and the mitigation of risks (Carlisle & Gruby, 2019). But this "third" family of governance systems (Rullani, 2009) includes other phenomena, like **networks** (Castells, 2004; Benkler, 2006), **platforms** (Srnicek, 2017; Constantinides & al., 2018), and **ecosystems** (Baldwin, 2018; Jacobides & al., 2018; Cennamo & al., 2018), all which in reality are **"meta-organisations"** (Gawer, 2014), characterised by porous and elusive boundaries (Parker & Van Alstyne, 2016; Berlinguer, 2023).

Overall, this new family of organisations has become increasingly important along with the development of the digital revolution and is progressively supplanting the organisational forms that characterised the Fordist era (Coase, 1937; Chandler, 1993; Jessop, 2015). This in turn points toward the emergence of a new typology of predominant governance models. (On this, see also section 5.4 and Box 17).

Yet, from another perspective, the increasingly widespread use of this matrix - especially in the form it has taken under the influence of the FOSS - can be associated with the practical rediscovery in the digital age of the predominantly **recombinatorial nature of innovation** (Shapiro & Varian, 1998; Arthur, 2009; Latour, 2010), iincluding its ambivalent relationship with standardisation (Blind, 2016; Hawkins & Blind, 2017; Garcia, 2018). This has in fact spurred a path in software-systems construction based on the reuse and the recombination of building blocks and modular components.[xliii]

A matrix to facilitate recombinatorial innovation?

BOX 13

It would be useful to explore the relationships between the increasingly widespread use of this matrix and the rediscovery of the predominantly recombinatorial nature of innovation.

The fact that the idea of a nexus between innovation and recombination has made its way through the digital revolution is not surprising. After all, **the ability to replicate and reuse any resource** - with enormous ease, at virtually no cost, and without diminishing its value or quality - **is intimately inscribed in the nature of digital technology**. It is one of its most essential attributes.

In recent decades, this approach to innovation has been developed from many different perspectives (Shapiro & Varian, 1998; Brian, 2009; Latour, 2010; Gawer & Cusumano. 2014; Hawkins & Blind, 2017).

In the cultural and artistic sphere, the practices of "meshing" and "remixing" have spread to many creative fields, indeed so much so that some speak of a "remix culture" (Lev Manovich; 2005; Lessig, 2008).

This is also how digital systems have been increasingly constructed: reusing and recombining already developed materials as building blocks. And on closer inspection, the principles of the matrix we are talking about – each of its principles separately and all together viewed as a matrix – seem to be made precisely to facilitate these recombinatory practices.

This recombinatorial approach to innovation has been also further expanded to embrace the theory that cyclical surges in growth depend on periods of combinatorial innovation of new interconnected technologies, the components of which are combined and recombined by innovators to create new devices and applications (Weitzman, 1998; Varian, 2010). Viewed in this way, this matrix and the recombinatory processes it fosters and promotes, also maintain a close relationship with other phenomena that have come to the fore in different streams of studies with the growth of the networked digital economy, such as those captured by the concepts of path dependency (David, 2007), network effects (Farrell & Klemperer, 2007), and increasing returns (Arthur, W. B. (1996).

This is because the underlying mechanism which is common to these phenomena is a process of decentralised aggregation along a development direction (Dosi, 1982; Hughes, 1989; Geels, 2002), which generate a multiplicity of externalities and synergies (Nelson & Winter, 2002; Perez, 2003).

Overall, these explanatory rationales can be summarised as follows. From a legal, organisational, technical, and economic standpoint, these principles: 1) lower costs and barriers to decentralised experimentation and innovations; 2) improve resilience, allowing an economic management of the costs and risks involved in a proceeding by trials, errors and adjustments; 3) make it easy and cheap to extend, integrate or recombine software (Berlinguer, 2021).

In practice, open source and modularity have grown in organic symbiosis in the development of software systems, each reinforcing the other. Both strategies have helped adaptation to the increasing complexity of software systems. In turn both also have operated as factors that have further increased this same complexity. The availability of – freely accessible, reusable and recombinable – OS components, together with the robustness that the FOSS ecosystem has progressively achieved, has spread their adoption, making them into essential building blocks in all software systems.

This re-usability, in turn, has incentivised further the development of modular and recombinable systems. On the other side, the scale and complexity reached by these systems and the widespread distributed nature of their production, maintenance and innovation, has made it increasingly unfeasible for any organisation, including even the biggest, to move independently, in isolation, developing private solutions by relying simply only on its own internal capabilities and technologies. This has, in turn, further strengthened this path of development.[xliv]

On the other hand, interoperability and standardisation have gained prominence in digital technology as means to simplify and speed up the growth of scale and the recombination and integration between systems or components, as well as the management of the complexity of the interdependencies that constitute these systems.

Along this same path, these architectural principles have become critical tools also for Big Tech firms' governance of their own digital architectures and of the ecosystems generated around the so-called "platform economy" (Berlinguer, 2018; Mazzucato, & al., 2021).[xlv]

The truly novel element is that public policy is also beginning to identify this matrix as a sort of new control grid. Looking at the EU strategy, we can speak of an incipient focus of technology policy and regulation on this matrix, recognising it as a lever for the governance of the design and architecture of the core components of technology systems, like platforms and infrastructures, and of the ecosystems of users, developers, and businesses that aggregate around them. As a matter of fact, we find these principles at the core of all the initiatives that the EU has undertaken with the aim of regaining influence on techno-economic systems in cloud computing (see Box 6).

However, government intervention at this level and by these means is a relatively new policy area. There are still uncertainties and fears in the way, and there is no simple recipe about how to handle this matrix. Innovations will certainly be needed to regulate and calibrate the use of the levers in the hands of sovereign powers and the public sector, so that they will be wisely and effectively used in these complex dynamic environments of technological development.

In any case, the modulation of this matrix is going to be an area for experimenting new policies for governing digital ecosystems. And, at this point, it can be argued that overall, the robustness of the trajectory underlying the success of this matrix would allow for governments to take bolder actions to tilt the playing field, as Carlota Perez would put it, toward specific directions of technological development (Perez, 2012). This could, for example, mean progressively introducing the use of open source components, open standards, and open APIs as binding requirements in critical core infrastructures, like for example, India's Digital Public Infrastructure initiative began to do.[xlvi]

5.3

NON-MARKET SYSTEMS AT THE CORE

Why does EU policy not take bolder such action? Various answers could be given. One of these is the famous fear of **"picking winners"**. Policy might adopt the wrong technology or the wrong technological path. True: one of the advantages of this matrix is that it significantly reduces the risk of lock-in and greatly improves flexibility and resilience in technology choices. However, it cannot completely eliminate such risks. All technology choices produce their own forms of path dependence, legacy and switching costs. In any case, this matrix provides the best recipes for addressing and wisely reducing these risks and, as the case may be, the costs of adjusting wrong decisions.[xlvii]

Surely, it would be necessary to design these decisions in a way that ensures maximum resilience and maintains pluralism and redundancy in choices (Benkler, 2016). Frankly, this is not an easy endeavour for public policy and public sector, as we know it.

Another reason for reluctance is the challenge of combining **rules-based governance** - as is appropriate and common for regulations, public authorities and public bodies - with the need to adapt any governance to a **highly dynamic technological environment**. This latter requires detailed, specific, and ever-changing technical knowledge, posing an unprecedented challenge for which regulations and public actors are unaccustomed and unprepared, and for which they necessarily have to rely on external knowledge and more flexible forms of action.

Again, this matrix provides the best approximation for this challenge, too, in terms of providing general principles and rules which could inform a rule-based governance. But the effective monitoring and ongoing implementation of these rules would remain a challenging task. The creation of many advisory bodies in the EU initiatives in the digital field (see Box 6, for cloud computing) reflects this necessity of an open and participatory governance for these initiatives. But the design and governance of an innovative kind of public agency (Florio, 2020) on these frontiers, remains an addressed task (see on this also the next section 5.4).

This is even more the case because there is another very important reason for the reluctance to fully adopt and apply this matrix of principles in public policy. This reason lies in the complex and partially idiosyncratic relationship this matrix has with intellectual property rights (IPRs) and markets. This characteristic is magnified by FOSS, which is a modern digital commons. But the argument can be generalised, especially insofar, as FOSS's **non proprietary model** has spread to the other principles, as we have been arguing.

Indeed, in a way it is surprising, when we consider that these principles of technological development already provide **most of the digital infrastructure** and predictably will do so even more in the future . What stands out, in fact, is that the core of these infrastructures is made up of components that - regardless of widespread business participation - **are neither produced nor governed by market systems** (see Figure 9).

Core Infrastructure

- Open Source Building Blocks
- Open Standards
- Open APIs
- Interoperability Rules
- Design Rules

Figure 9

This peculiarity is probably one of the main blind spots of current European policy, which continues to be almost exclusively oriented toward the creation and facilitation of markets. This means that it largely overlooks or underestimates the issue of the **governance** of these **non-market systems** of innovation, technological development and maintenance, in both their political and economic aspects.

Here, we can limit our analysis to the economic aspects. In economic terms, FOSS, standardisation, modularity, and interoperability highlight and incorporate a plurality of economic principles. If you focus on markets alone, you risk neglecting the core of these systems. Markets represent only one ordering principle, which is often not the core one. Rather the main relationships of these principles with markets can be described as twofold. On one side, their application has the dual effect of **eliminating and creating markets**.

They typically eliminate competition in certain technological stacks, precisely where they operate, often instead unleashing it in other adjacent or complementary areas. Indeed, the control on the shaping of this dual impact has become critical in the uneven distribution of opportunities and costs, gains and losses in digital ecosystems and networked economies. This is a dual shaping power that Big Tech firms have become skilled at exploiting and utilising (Berlinguer, 2018).

On the other side, beyond this dual shaping power, there is another peculiar relation which they maintain with the market. These principles directly generate usable resources, productivity improvements, saving of efforts , and innovation opportunities, in multiple different ways. In a word: they **directly produce wealth**. Yet this wealth generation occurs through forms and in ways such that the bulk of the value that they generate is shared, cannot be appropriated in an exclusive way, and is not directly measurable with market transactions. One consequence is that these processes of value generation, circulation and appropriation remain largely invisible to economic accounts (see Box 14).

The Value of sharing

BOX 14

How much is FOSS worth? It is very difficult to answer this question. Why? Because most of the value of FOSS leaves no trace in corporate balance sheets, consumption indices or GDP. FOSS production was initially entirely voluntary and unpaid. Today, voluntary contributions remain an important component, but likely the majority of FOSS is produced by companies and by developers paid by them. Even so, FOSS maintains a central characteristic: as such it is not and cannot be directly marketed. Its circulation and consumption do not produce monetary transactions. And thus its value is not calculable by current economic-value measurement systems (Berlinguer, 2016).

This is, in fact, hardly an isolated phenomenon. Economic accounting systems are blind to many other important and relevant phenomena with respect to the functioning of the economy. The multiple criticisms that have accumulated around GDP – the main official measure of the economy – bear witness to this (European Commission, 2009; Brynjolfsson & Saunders, 2009; Fioramonti, 2013). The FOSS case is, however, a very interesting and paradigmatic case in many respects. Software is the main technology of the digital revolution. As has been said, software is eating the world. That is, increasingly in all sectors, processes and activities are being "softwarised" – that is, empowered by or delegated to algorithms. But today, to say "software" largely means to say FOSS. This means that the current financial, monetary and economic **accounting system shows a structural blindness towards one of the central phenomena** of the ongoing digital transformation.

Recently, the EU Commission funded pioneering research that tried to answer the question: how much is Free and Open-Source Software worth to the European economy? The research produced interesting results. It has estimated that EU companies invest around €1 billion yearly in open- source software, and that FOSS has a positive impact on the economy of between €65 and €95 billion. The study also estimated that an increase of 10% in contributions to open-source software code would generate an additional 0.4% to 0.6% GDP annually and promote the creation of 600 additional start-ups (Blind & al., 2021). It must be said that these estimates are based on unconsolidated methodologies. In general, giving a value to non-market goods, including public goods, has always been a difficult and neglected Issue in economic accounting.

But in truth, there is something more radical at stake in the challenge of measuring the value of FOSS. The salient point is that many of the ways of creating and appropriating value that characterise FOSS as an economic good not only escape the conventional metrics by which economic value production is measured, but are structurally different from the mechanics of exchange value. Several years ago, Steve Weber proposed the concept of "**anti-rival good**" for FOSS: a neologism to describe the peculiarity of some of these modalities (Weber, 2004). A rival good is a typical material good, for example an apple or a barrel of oil, which can be consumed only once and in each portion by only one consumer. The electric lighting of a street or a television broadcast are, instead, examples of non-rival goods: they can be consumed simultaneously by several people, without anyone seeing their value being reduced. An anti-rival good is a good that **increases its value through its sharing**. The more people use it, the more its value increases for everyone. This is a counter-intuitive phenomenon, which Arthur captured with the notion of "increasing returns" (Arthur, 1996). The value of FOSS - but also for example that of social networks or standards - often has this characteristic.

More generally, in explaining the FOSS economy and its system of producing and circulating value, market and monetary economics is certainly important, but it is not able to adequately and fully account for this phenomenon. This has been partly discussed and studied in relation to the motivations of developers early in the history of FOSS, when communities were predominantly made up of volunteer contributors. These studies demonstrated how directly economic motivations were inadequate to account for the plurality of mechanisms that supported the developers' contributions.[xlviii] But this is also true today in relation to the FOSS economy as a whole. To represent it adequately, a broader and more plural conception of economic processes is needed. Many modes of value production, circulation and consumption that are involved in this economy require a revision of both conceptual and measurement systems to be adequately measured. A few years ago, other pioneering research funded by the EU Framework programme FP7-ICT proposed to evaluate the value of projects based on community forms of regulations and the production of digital commons, in order to integrate monetary values with alternatively conceived value indicators (Berlinguer, 2016; Fuster & al., 2016). For example, the quantitative indicators proposed included: "community building", "social use value", "reputation-social capital", "mission accomplishment", and "ecosystem derivative value". Furthermore, it also experimented with new methodologies for the quantitative measurement of value through the use of digital metrics. This latter remains a new path that has still been insufficiently explored, but which could help to profoundly transform our way of representing and regulating economic processes. In fact, the progressive embodiment of social flows upon digital substance is generating a new "datascape" (Latour, 2010), that is radically transforming our perceptions about what was until recently considered intangible, immaterial, invisible, as well as private and intimate as opposed to public and measurable. Accordingly, this "materialisation" of previously intangible spheres - or rather the materialisation of new "digital objects" (Rogers, 2015) related to spheres that were previously considered intangible - is generating the possibility of new **quantitative practices**, upon what was thought until recently as intractable by calculative devices (Berlinguer, 2016).

It is also interesting, in this regard, that the problem that we face in the case of FOSS is not much different conceptually to that concerning the other principles of the matrix. For instance, with regard to standards, whose value has rarely been explored, and which operate according to a logic not unlike FOSS (Kindleberger, 1983; Blind & Jungmittag, 2008; Sidak, 2016). The same is true of the benefits and costs of modularity (Langlois, 1997; Baldwin & Henkel, 2012) and interoperability (Haile & Altmann, 2018). These are even more elusive topics, and approaches to the measurement of their value or impact are still less mature. Nevertheless, interest in new forms of quantifying and measuring these value-generating mechanisms is likely to grow with the data economy. (see Figure 10).

Figure 10 — How standards and interoperability eliminate and create markets and generate productivity

There is also a corollary to this feature, which is more "political", at least in a broad sense. The main economic device through which these principles generate value is **collaboration**, **not competition**. This includes, a considerable and growing extent, indirect forms of collaboration (e.g., by design or by side-effect). Indeed, this is a common function of these principles: that they facilitate collaboration **among people and organisations with weak or nonexistent ties and different or even competing interests and agendas**. Or, as Powell would have put it, under conditions in which "neither markets nor hierarchies" provide effective means of promoting collaboration (Powell, 1990).

The growing importance of this matrix is, therefore, clear evidence that in order to analyse and govern contemporary digital techno-economic ecosystems, one needs to acknowledge that they are the result of the interaction of different regimes of ownership, governance, and value generation and appropriation (Berlinguer, 2018). This hints at a new kind of mixed economy, or at the simultaneous working of a plurality of principles of "economic integration", as Polanyi would have called them. He summed these up in three ordering regimes: reciprocity, redistribution and market exchange (Polanyi, 1957).

EU policy has only begun to address this issue. For example, it centres its initiatives in cloud computing in these "**pre-competitive**" areas of technological development.[xlix] Similarly, this issue is present in the EU's last regulations on data, which aim to facilitate both markets and sharing in data economy and data exploitation. Yet - beyond mechanisms of unrewarded sharing and markets based on the private ownership of data - there is no adequate consideration for what would be the third pillar in Polanyi's approach: centralisation and redistribution. There is no clear economic governance of the systems which generate shared value, and no clear system of fair distribution for their often-contradictory effects.

This lack of consideration and of fair and effective governance creates many problems. To paraphrase the feminist philosopher Fraser, this invisibility generates problems of justice-redistribution, misrecognition and lack of representation (Fraser, 2017).

The clearest example is provided by the concerns which are currently exploding around the security of these systems. In their intricate complexity they sometimes conceal unexpected systemic vulnerabilities. These latter are the result of unknown dependencies, on the basis of which sometimes millions of organisations, including the world's largest governments and corporations, opportunistically take advantage of the precarious and voluntary labour of a handful of developers (see Box 9). But the implications of this plurality of economic principles are much broader, and with the growing importance of these mechanisms of value generation - also beyond software[l] - they are headed to becoming more impellent (see Box 15).

Overall, an organic consideration of its importance could lead to new approaches in many areas, such as the fight against dumping and monopolistic strategies, fiscal policies, the financing and provision of public goods, and even economic accounting metrics. But broadening the perspective further, this issue revolves around a system of economic regulation of a different nature than the one built around the Fordist-Keynesian paradigm (Jessop, 2016; Perez, 2003). The ability to fully exploit the potential of the digital revolution may depend significantly on the establishment of this new type of regulatory regime, (see Box 17).

On a more immediate and practical level, recognising the central importance of these mechanisms would help thinking about the development of an autonomous European digital industry in new ways. This would mean explicitly putting these essential common components and their governance systems at the heart of any digital industrial policy, rather than reducing the latter simply to a matter of companies and markets.

Catena-X: What Governance for Industrial Data?

BOX 15

One of the main objectives of the EU digital strategy is to gain a leadership position in the next era of exploiting industrial data. However, the path for such exploration is long and yet to be figured out, and it is still too early to know how this exploitation will work. The EU introduced the idea of "dataspaces" as a preliminary and facilitating infrastructure and organisational framework, necessary to facilitate the experimentation of use cases of data markets and concrete applications. The main issue and complication is that the data to be exploited often needs to be shared across many different actors.

This experimentation first began in the automotive sector. The pilot project is called Catena-X, financed by the German Ministry of Economy and created in close connection with Gaia-X. From the beginning, the project involved the main German car manufacturers and the component suppliers in the automotive supply chain, but it is also intended to be open to car manufacturers from other parts of Europe and the world.

Catena-X is exploring use cases for data, particularly around the traceability of parts and components along the value chain and from raw materials to recycled material.

Catena-X is also an illustration of the fundamental role that the matrix of principles which we have discussed - open source, interoperability, modularity, and standardisation – could have for building data infrastructures.

These principles are applied to build the fundamental layers of the technology (see also Box 6) and to shape the rules that should foster the necessary trust of stakeholders, ensuring security and control ("sovereignty") over their data, freedom from lock-in strategies, and ease of building applications. The expectation is that markets will be built on these foundational layers. But we should not be surprised if in the future of the data industry we see non-proprietary systems occupying a fundamental role, similar to what has happened in the case software.

Certainly, in these early stages, something is clearly apparent. That is, a "radical collaboration" – and this is the slogan adopted by Catena-X – across the industry is central to this effort. (see Figure 11) This is another example of how collaboration takes precedence in the challenges that await governance in digital transformation.

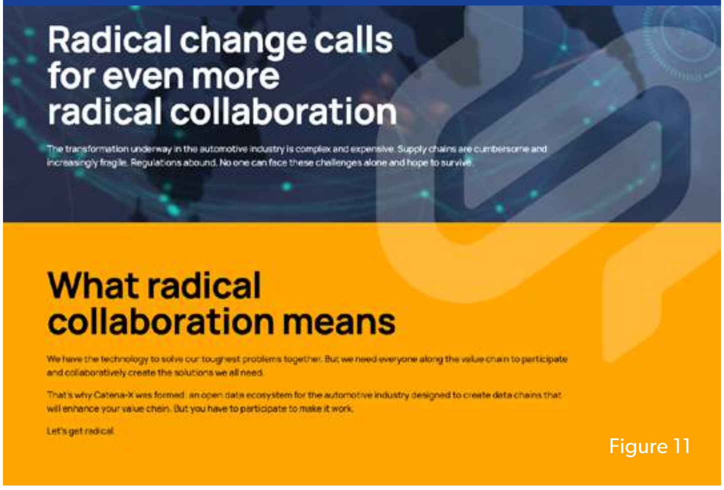


Figure 11

5.4

GEOPOLITICS AND THE NEXT GENERATION OF HYBRID GOVERNANCE SYSTEMS

The increasing complexity, dynamism, integration and interdependence of digital systems - which is one of the reasons for the success of this matrix of architectural principles - also exert constant pressure on the direction of innovations in the governance of these systems. Furthermore, as the importance of these principles of technological development grows, there will be increasing pressure more explicitly to address the blind spots of existing governance systems. Indeed, if we look at the role played by FOSS, standardisation, modularity and interoperability in digital technology, these are all principles of organising technological development that have gained greater importance in the last two-to-three decades. But along with this rising importance, the governance of each of these systems has also evolved (Berlinguer, 2020a; 2021).

And although it is difficult to generalise, it is fair to say that, in the current phase, each of these systems is in its own way called upon to introduce innovations to cope with the growing complexity, integration and dynamism of digital systems. And it is also fair to say that, at another level, they are called upon to adapt their governance and effectiveness to the essential role that digital systems play in the most critical daily activities and infrastructures. The widespread centrality of these systems, their critical role, and the scale and scope of the interests involved, are also what drives governments to intervene in their governance.

This brings us to a second, more "political" and "**evolutionary" perspective** (Hughes, 1987; 1993; Geels, 2002; Berlinguer, 2023) from which to interpret the growing success of this matrix of principles in the architecture of digital systems and to inquire about the next challenges that its governance systems will face.

In this case, the focus must be on the agents who have grappled with the development of these systems. How they struggled to introduce innovative solutions, how they succeeded in producing innovations in previous regimes and habitual ways of doing things, and how they progressively transformed or supplanted them (Geels & Schot, 2007; Geels, 2010; Berlinguer, 2020a).

Again, Free and Open-Source Software as a movement and ecosystem offers the best example of this type of explanation. In fact, in its journey it is easy to identify two different phases, from this point of view. FOSS first emerged among voluntary communities of developers, and in this first phase, the motivations of individual developers were the main driving force. The main dilemmas of FOSS concerned how to effectively organise collaboration among dispersed people, with different interests and motivations, in the absence of hierarchical ties and market exchanges. We may call this the "heroic" phase of **Free Software**, which created and consolidated the institutional, organisational and cultural innovations that are still the basis of FOSS today (Bauwens, 2005; Benkler, 2006; O'Mahony, 2007).

The second phase, on the other hand, was characterised by the market adoption of FOSS. In this phase, the initial dynamics were complemented and increasingly overcome by new driving forces, represented by the adoption of FOSS by business, and the new competitive dynamics and business models that have characterised the growth of the digital economy and the emergence of a new type of capitalism. These dynamics have been influenced by FOSS and its distinctive features, but they have also profoundly changed the characteristics of the FOSS ecosystem itself. This can be called the era of **Open Source** (see Box 1). During this phase, hybrid arrangements have gradually emerged. On the one hand, the logic of FOSS as a digital commons, and the dialectic it brings with it of both destroying and creating markets, has installed itself at the centre of the digital economy. On the other hand, corporations and Big Tech have gradually gained primary influence over the FOSS ecosystem.

A new culture has spread from FOSS to the most innovative technological sectors, and new organisations and infrastructures have grown up and consolidated this evolution, through powerful foundations and software- development platforms (Riehle, 2010; Hunter & Walli, 2013; Izquierdo & Cabot, 2018; Berlinguer, 2020a; 2023). These hybrid arrangements have managed to dynamically maintain contradictory principles, such as private profits and sharing, communities and businesses. But it is also true that at the end of this second phase - where we are now - the FOSS ecosystem appears to be crisscrossed by unresolved and uneven issues of sustainability, fragmentation, security, and equitable distribution, which can only be addressed by interventions in the **governance** systems **on a larger scale**.

However - and this is the point - at this juncture, EU digital policies on cloud computing signal that once again the most influential forces behind the development of FOSS are changing. They signal that a third phase of development is beginning and that the next phase of evolution will be characterised by increasing government intervention in the dynamics of FOSS, as well as in the governance of the design of architectures for standardisation, modularity and interoperability of critical infrastructure. This is evidenced by recent developments in government policies, and not only in Europe. In fact, it would be easy to point to similar initiatives taking place, for example, in China, India and - in different ways - in the United States (Arcesati & Meinhardt, 2021). All major governments are increasingly turning their attention to FOSS, trying to figure out how to exploit its possibilities or reduce its risks.

This increasingly **direct involvement of governments** is likely to have a profound impact. And it is plausible that the FOSS ecosystem is about to experience an evolution as radical - and difficult to predict in advance - as that seen in its early stages. But we can see one thing already. Along this evolution a new type of hybrid organisations is going to emerge. Looking at the case of the EU, we can see many embryonic and tentative examples that this is the direction in which new governance systems are heading. We can call these organisations **"second-generation hybrids"**, because in very broad terms, these organisations, policies and systems of governance will have to grapple with an innovative "tripartite system of governance" (Berlinguer, 2023), in which the logics of voluntary communities, the pursuit of profits in the markets, and the instances and powers of states will have to adapt, intertwine and recombine in new forms.

However, while we know a little more, at this point, about the relationships between commons and markets, communities and enterprises, we know much less about what an organic, effective governmental policy, integrated in a non-proprietary system of technological development, could look like. There is no blueprint or model of success, here.[li] Cloud computing, as the most mature techno-infrastructure enabling this new phase of development, is probably going to pave the way for this more organic involvement of governments, public policy, and the public sector.

In theory, it can be thought of as an opportunity for governments, markets and communities to learn how to compensate for the relative weaknesses and failures of each system (Benkler, 2013; Berlinguer, 2021). But these new initiatives, of course, could just as well generate failures and bring together the worst of each system. It may be predicted that innovations and adaptations will have to take place simultaneously in each of these systems of governance. The urgency of ensuring the security of these complex systems is going to make this the first field of application of this tripartite logic. The alarm in the FOSS community over the EU's recently proposed Cyber Resilience Act is an example of how things could take a turn for the worse (see Box 9). But perhaps the most important and significant challenge will be the impact of the geopolitical conflicts that are erupting around the control of the next generation of technologies. Looking forward, geopolitical tensions and security-related pressures are likely to influence and change the Free and Open-Source Software ecosystem and the principles of open innovation and open standards in unpredictable ways (see Box 16). At first glance, one may even observe that FOSS – which is, by its legal nature, a global commons - has traits idiosyncratic with regard to divisions of national sovereignty and geopolitics. It may thus be in danger of being swept away by geopolitical and security imperatives (Pannier, 2022). However, if the past trajectory of FOSS teaches us anything, as happened with private property and markets, the arrangements that will emerge will be probably more nuanced, articulated and "layered." Above all, it is unlikely that the FOSS ownership regime is going to retreat in favour of a return to proprietary software, especially in the more infrastructural levels of the technological systems. Rather, FOSS is likely to become a competitive lever also in this new development phase of the digital revolution. **A competitive lever in public and industrial policies**, in growth and development strategies, and in the political and geopolitical struggle to assert a new kind of "sovereignty", or rather leadership and mastery over future techno-economic systems (Berlinguer, 2023).

Otherwise, in certain cases - as suggested at the presentation of the European Digital Commons Initiative, promoted by the French presidency of the EU in 2022[lii] - the convergence around FOSS solutions could help to reframe global interdependence on new bases. That is, in terms of shared solutions allowing for autonomy, sovereignty, security and even the localisation of production, in non-antagonistic forms, instead maintaining terrains of joint collaboration and greater transparency; as a linchpin of a "non-rival technological sovereignty", as suggested in Paris, or of "a non-aggressive European geopolitical strategy", suggested in another context (Lapenta, 2021). Indeed, this is what is suggested by the India's Digital Public Infrastructure (DPI) proposed at the G20 as a model for global development.[liii] In either case, FOSS and its rationale will most probably be an essential component of future international standards in cloud computing, as well as in the other emerging digital technologies. And this will require that governments and public sector organisations learn to cooperate in radically new ways.

The European Union's plans in its cloud-edge-IoT strategy, which will make broad use of FOSS and open standards, point in this same direction. Likewise, it is the path toward which the governments of China and India seem to be leaning. Still, it cannot be ruled out that the US government could, conversely, be tempted to try to impose restrictions on FOSS in order to defend its technological advantage, for security reasons or as part of its containment against China catching up[liv] (see Box 16).

Interestingly, looking back in time, this trend would not be ever so new. It occurred repeatedly at key stages in the rise of FOSS adoption in the market: the first companies to take up the challenge of betting on FOSS - and its challenging features - were in fact often the companies that had fallen behind and were trying to catch up. The difference this time is that the nature of the competition and the innovations in governance models will take place at a much larger scale, will involve the mobilisation of state powers and **will inevitably be highly political**.

FOSS and sovereignty: a difficult relation?

BOX 16

How will the relationship between state sovereignty and open and collaborative innovation evolve?

This is one of the questions that will most influence the digital innovation scene in the near future.

FOSS is often described as a tool to regain sovereignty. And for good reasons. FOSS is freely available, reproducible, editable; it is transparent, and it is royalty-free. All these features make FOSS a tool that increase autonomy, freedom and control over software systems. However, there are also idiosyncrasies between FOSS and sovereignty, and the thrusts toward deglobalisation, geopolitical tensions, and government policies that aspire to use FOSS as leverage for "sovereign" policies of technological innovation and development are putting **increasing pressure on the FOSS ecosystem** (Pannier, 2022; Berlinguer, 2023).

One of the first signals has been the migration of some **FOSS foundations**. The Risc-V and Eclipse foundations, for example, moved from the USA to Switzerland and Brussels, respectively. And in Europe, a Linux Foundation was created, autonomous from the parent foundation based in the USA. The reasons are different in each case, but the shared backdrop is geopolitical pressures and governments' increasing interest in FOSS. Even more remarkable is the creation of FOSS foundations in China, like the OpenAtom Foundation. In China, the goal of achieving a leadership position in the FOSS world has been made explicit in government policy and programmatic documents.[lv] Equally significant are the ongoing movements around open-source development **platforms and repositories**. Again, the Chinese have been pushing toward the development of their own platforms[lvi] in order to shield themselves from geopolitical risks. The blocking of access to the GitHub platform to Russian developers after the invasion of Ukraine reinforced this trend.[lvii] India also has an ambitious plan on FOSS[lviii] and has, under government direction, developed a Digital Public Infrastructure - a group of FOSS basic building blocks for digital systems – that is now pushing as global standards through the G20, the ITT and the UNO. Meanwhile, in Europe it is becoming common to talk about "**European open source**", as opposed to open source "controlled" by US Big Tech companies (Martí, 2022).

Just as open source is a protagonist **across all the frontiers of digital innovation**, so are the tensions coming from government intervention. Microchips provide a good example. Several US legislators have expressed clear concerns about the Risc-V open-source project in microchip design and expressed their intention to ban US developers from participating in it.[lix] Meanwhile, the Risc-V foundation, whose members include many Chinese companies, has moved from the United States to Switzerland to avoid being dragged into these geopolitical battles.[lx] But things can also go the other way, too. For example, in the case of 5G, where the technological advantage is Chinese, US industry and government are sponsoring open-source solutions such as the 5G open RAN.

Another area to pay attention to is Artificial Intelligence. Lawmakers are just beginning to grapple with AI. The issue is not just about politically controlling access to the latest technology. There is a broader issue of regulating a technology that has enormous potential impact on the totality of human activities. In any case, many of the best projects are going to use open sourcing important stacks of their AI models as a competitive strategy, in an effort to promote adoption, attract developers and accelerate innovation. Moreover, in addition to competitive dynamics, pressures are also growing in AI to make algorithms and the data used to develop them transparent, for a variety of economic, cultural, social and political reasons. This further contributes to the push toward the adoption of open-source solutions. The EU AI Act, for example, is probably going to introduce a positive exception to the regulation for open-source AI models, which would be justified by the greater transparency, openness to competition and democratisation that open-source solutions provide.[lxi]

However, if FOSS solutions lower barriers to the accessibility of the most advanced models of AI, they also destabilise any policy that attempts to limit the export of the most advanced technologies, and thus geopolitical control over their use. Moreover, more generally, they can weaken the effectiveness of any kind of regulation.[lxii] Indeed, some argue that the scaremongering around the dangers of AI is fuelled by Big Tech companies themselves in order to impose strict regulations that could create barriers to open source and thus eliminate their main source of competition.[lxiii]

How, then, will the relationship between FOSS and sovereignty evolve? Will we see FOSS destabilised and **cornered by a return of states, geopolitics and security concerns?** Are we moving toward a **fragmentation of FOSS** into different "sovereign" or geopolitical blocs? Will we see a **political competition around the strategic use of FOSS** through the enhancement of its logic and culture and a policy of attracting FOSS developers, projects, foundations and platforms? Or will we see FOSS provide a **model for the collaborative development of global public goods** and inspire a different kind of globalisation path? In the abstract, **these are all possible evolutions**. What is more, they can also coexist, giving rise to several possible combinations.

What we can observe at this stage is that these tensions and innovative drives in the relations between FOSS and state actors are the result of the conjunction of several processes. First, there is the evolution of the FOSS ecosystem and the systemic and infrastructural role that FOSS has come to play. This evolution puts stress on current arrangements, pushes for developing systems of governance at a broader scale, and pulls public actors into the governance of the ecosystem. Second, the digital revolution has reached a stage of full maturity. The impact of digital technologies that are in the course of being designed and deployed has a scale and scope that pushes public actors and policy to intervene in their governance. Third, the crisis of neoliberalism and the intensification of international competition are causing a strong return of public intervention.

Looking backward, however, it is worth remembering that a similar idiosyncratic tension also appeared early in the history of free software: a tension between FOSS and markets. For the vast majority of managers, in the digital industry itself, the logic of collaborative, non-proprietary innovation was a source of doubt, fear and uncertainty. It took the emergence of a new generation of entrepreneurs and managers imbued with this new culture for new combinations to be invented between FOSS and commercial enterprises. Today, these hybrid combinations are prevalent and powerful on all frontiers of digital innovation.

Thus, perhaps to see convincing answers to these questions emerge, we will have to wait for the emergence of a new generation of political ideas. Where should these ideas dig in? If we were to build on the trajectory that has led this matrix to progressively prevail, there are **two general principles** and values that seem to have **asserted their primacy**: namely, **freedom to action and collaboration**. How are these principles reconciled with the classical notion and praxis of a sovereign state? Looking at how little the EU countries have been able to cooperate so far, it would seem that the answer is not a simple one (On this, see also Box 17).

CONCLUSION: STRUGGLING FOR AN INNOVATIVE GOVERNANCE SYSTEM

Here, we can summarise the long journey that we have taken, and the pieces that we have put together in this essay.

A new generation of general-purpose technologies and enabling infrastructures are in the process of being designed, developed and deployed. Cloud computing, the Internet of Things, 5G, and Artificial Intelligence form the core of this group of new technologies. They are set to develop in a highly integrated manner and will have a profound and far-reaching impact on all social and economic sectors, as well as on the functioning of all types of organisations and institutions. Taken all together, they mark the entry of the digital revolution into a new phase.

Against this backdrop, the EU is trying to use this moment of change as an opportunity to re-enter a "race" for digital transformation, in which it has so far failed to participate as a major player. Or at least it is trying to avoid an irreparable worsening of its technological dependence on non-European monopolies, which have come to largely dominate the digital economy, in turn potentially jeopardising the EU's future autonomy, security and prosperity.

The EU's endeavour takes place in a new political climate characterised by growing security concerns, intensified international competition, and the return of interventionist and protectionist policies by governments, especially in the most advanced technologies. All this compels the EU to rethink its *laissez faire policy*. The EU also has to deal with its specific political status of being made up of a Union of states, and it has to struggle with the absence of a strong autonomous digital industry. These conditions have, perhaps, facilitated a more assertive use of regulatory leverage. But on the other hand, they demand that solutions be sought that are not easy and that must necessarily be innovative.

In this essay, we have focused on the EU's policy regarding cloud computing, which is the most mature of the new infrastructures being deployed and has been the subject of numerous EU initiatives and legislative interventions.

In the first part, we provided an overview of the main features of cloud computing, its foreseeable impact and the increasing size, complexity, dynamism and integration of the last generation of digital technologies. In the second part, we reconstructed the evolution of the EU's approach to digital policy and the main initiatives undertaken in the field of cloud computing, devoting special attention to plans for the migration of the public administration to the cloud.

The absence of an autonomous strong digital industry in the private sector forced the EU to undertake a strong industrial policy. Through a partial exercise in abstraction, we tried to outline a possible comprehensive strategy. This strategy would fundamentally be based on a bold and strategic use of FOSS and open standards, and would be supported by regulations and coordination at the European level.

In essence, it would be based on the main existing - and the most predictable future - trends in the evolution of the last generation of digital systems. However, while it is obviously too early to judge the effectiveness of the new EU cloud-computing policy, as we have remarked, the first steps of its implementation are not encouraging. To cite only the most obvious reasons, EU cloud computing policy seems to lack political determination, adequate investment of resources, policy clarity and coordination among national governments, and a unified agency to overcome the fragmentation of existing governance.

Nevertheless, it is undeniable that EU policy in cloud computing marks a change of trajectory in European digital policy and it has put together innovations around the construction of new instruments of political governance of the new generation of digital infrastructures. The most obvious example is in the regulatory field, where the EU is leading the way in several areas and is set to exert global influence. But there are other innovations in the EU's cloud-computing strategy that deserve further study and could produce further developments in the future. In the last part of this essay, we have chosen one of these policy innovations. This means the identification of a matrix of principles of technological design and development to which to entrust the building of cloud infrastructures: namely open-source, standardisation, modularity, and interoperability.

We have framed these principles as a matrix, and we have explored its rationales and characteristics. Our intention was to uncover some of the characteristics that can be glimpsed behind many of the initiatives undertaken in EU cloud policy, and which may also have broader significance in the search for new governance models for the incipient new phase of digital transformation which we are entering into (see Box 17).

In this way, we have come to identify three main areas of innovation in the political, economic and technological governance of cloud-computing technologies. Innovations along these lines emerge in many features of the EU's ongoing initiatives. Yet it is fair to say that they are still insufficiently recognised and even less placed at the centre of the EU's vision and strategy. Instead - this is our conclusion - the challenges that they represent are set to become important in the current resumption of public intervention in digital policy and could determine in significant measure the success or the failure of EU policy.

In conclusion, let us summarise these areas that we have been discussing - and what they suggest in terms of where we should expect public policy innovations in the near future.

Firstly, these principles are already widely used in industry and by the largest digital companies, as critical tools to build their technological systems and orchestrate and shape their business models. What is new, here, is the use of these principles as a lever for public policy. One of the characteristics of this matrix is that they create and eliminate markets. That is to say: they shape markets, but also eliminate them and unleash productivity according to a different logic (Berlinguer, 2023; Mazzucato, 2023). As EU initiatives themselves show, the use of this matrix can head in two different directions.

It provides tools to disarticulate the monopolistic systems that have established themselves on the Internet and in the digital world, and to create more space for competition and innovation. And they can function as aggregative principles for the collaborative development of new systems. At least in theory, this is also true at the political level. In this way, they provide a compass for the convergence of different EU states. In any case, looking forward, the question of ***how to wisely use the powers in the hands of the public sector in the modulation of these principles, wielding them both boldly and intelligently, is going to be one of the most critical areas of experimentation for public policy***.

Secondly, we have argued that there are multiple forces at work behind the increasing importance of this matrix of principles. However, one of these is the growing complexity of digital technological systems, and this complexity also reverberates on their governance, which has in fact continuously evolved over the past two decades. What the EU policy suggests to us is that a new type of organisation is beginning to take shape to meet the challenges and characteristics of the new phase which we are entering into. We have framed these new organisations as a "second generation" of hybrids. The first generation is the one which emerged from the dynamic hybridisation of communities and businesses, commons and markets.

The novelty, in this second case, will come from the full integration of the public sector in these governance systems. Looking forward, we can anticipate that ***an important part of the innovations that will accompany the next generation of public policy will play out around the governance of this new generation of hybrid organisations***. Although we are seeing the first embryonic examples in some European initiatives, this is probably the least considered and the most important of the challenges ahead.

Finally, there is a third feature of this matrix that proposes several challenges with regard to the political and economic governance of future digital systems. This feature is emphasised by FOSS as a digital commons that has grown up at the centre of the quintessential technology of the digital revolution. But the argument can be generalised to all the principles of the matrix, especially as they are increasingly intertwined with FOSS itself and its non-proprietary nature, as we have argued.

All these principles are based on a ***collaborative logic***. This is not necessarily deliberate. It is not necessarily grounded in common goals. But essentially, the core value that they produce is generated by a logic of convergence, alignment and sharing. As we have argued, one of their common features is that they facilitate a dynamic coordination and division of labour that is based neither on hierarchy and top-down planning, nor on price signals and market transactions. This, in turn, indicates a change in the dominant organisational forms (see Box 9 and the previous point). But digging even deeper, it signals the ongoing installation of a new mode of growth or development (see Box 12).

There is no doubt that the importance of this logic has so far been largely obscured by the neoliberal "fixation" on the centrality of markets and competition. However, as the importance of these value-generating systems grows, in conjunction with the maturation of the new paradigm, this neglect will become increasingly untenable. On the contrary, **addressing it explicitly may uncover possibilities for radically rethinking a broad spectrum of policies** in the transition to cloud computing and, more broadly, in the next phase of digital transformation.

Toward a new model of development?

BOX 17

Several authors have worked around the concept of "paradigm shift" in order to frame and understand the innovations produced by the digital revolution. These include Manuel Castells, with his theory of **"informationalism"** (Castells, 2004), and Carlota Perez, with her theory of **"techno-economic paradigms"** (Perez, 2003). Both see the eruption of a sequence of interconnected radical technological innovations as the main driving forces behind these paradigm shifts.

It is certainly more than plausible that we are in the midst of a mutation of this nature. One of the most interesting implications of their theories is the idea that these changes of paradigm introduce discontinuities and novelties in the **forms of growth** and in development modes. From this point of view, the challenges that emerge in the construction of new political, technological and economic governance tools in the transition to cloud computing potentially take on a broader meaning, as they can be framed within a paradigm shift in the forms of government and in the very conceptualisation of growth and development.

There are many indicators that a shift of this kind is underway. For example, it is known that there is a dissociation - a mismatch - between the flows of production, consumption and capitalisation in the digital economy (Brynjolfsson & Saunders, 2009) and the systems for measuring economic processes developed during the Fordist-Keynesian paradigm, such as GDP, an indicator introduced to govern the economy at a macroeconomic level in the 1930s and '40s (European Commission, 2007; Fioramonti, 2013).

The explosion in the importance of "intangibles" - assets that have an importance in the production of value but which lack a conventionally shared measurement (Arvidsson & Peitersen, 2013) - or the so-called productivity paradox - the difficulty of recording increases in productivity resulting from ICT - that economists and historians of technology have been debating for three decades (Van Ark, 2016), are just some of the examples that can be given.

FOSS itself can be taken as an emblem of this dissociation. As we observed (see Box 14), tthe measurement of the value produced by FOSS remains a black hole. More generally, the growth of a new type of commons on the frontier of the digital revolution is perhaps one of the most striking novelties of the ongoing paradigmatic discontinuity (Berlinguer, 2020a). For the success of this innovative model of organising production occurred within the core technology of the digital revolution.

Despite its anomalous and even idiosyncratic characteristics with respect to private property and the market, FOSS has gradually established itself at the centre of the digital economy. Like other central phenomena of the digital economy, it escapes conventional economic measures. Finally, because it provides a model that is spreading in other areas, with microchip design and data as the most significant ongoing examples.

But, more precisely, beyond FOSS, the matrix as a whole could have a broader and paradigmatic meaning for the forms of governance that will emerge in the future.

Many of the characteristics - scale, complexity, dynamism, interdependence, integration, polycentricity - that pose challenges for cloud computing governance and that have brought this matrix to pre-eminence in software are actually challenges that cut across many other areas of technological, economic and political innovation. Moreover, it is realistic to expect that with regard to data governance we will see solutions modelled on this same matrix emerge (see Box 10). And it is not surprising that discussions have begun about the need to reach a new social pact around data management and governance.

One of the fathers of the concept of paradigm shift was the philosopher of science Thomas Kuhn. One of Kuhn's most fascinating contributions was his modelling of the cycle of phases that characterise the crisis and the replacement of a dominant paradigm in the context of "scientific revolutions". Carlota Perez borrowed the concept of paradigm from Kuhn and applied it to the techno-economic field (Perez, 2012). A paradigm should be understood as a **standard** and prevalent **way of "framing problems and providing solutions"**. Standardised mass production, the hierarchical division of labour within large vertically integrated companies, and the sharp division between planning and execution, are all exemplary of the paradigm that prevailed in the Fordist era.

Carlota Perez, in her theory, also modelled different phases in the sequence of a paradigm shift. Indeed, some of the challenges that we have seen emerging in the European attempt to develop a new governance capacity in the development of cloud computing systems can be framed within her theory and, following this approach, they signal a phase shift. Perez, on the basis of the cycles that have characterised previous "technological revolutions", argues that the full realisation of the growth and development potential of any new techno-economic paradigm requires overcoming the phase dominated by *laissez faire* philosophy and the prevalence of finance in the governance of the economy. These are both - according to his theory - typical features of the early stages of technological revolutions.

Perez also argues that the return of the primacy of the "real economy" coincides with a **restructuring of the forms of political government** which, in his model, is typically the last level to be affected by the technological revolution (Perez, 2004; 2013). This ultimately leads us to see that the re-foundation of a capacity for the political governance of technological and economic processes, adequate to the challenges of the digital age, is one of the most pressing unresolved challenges of the current phase of political and economic impasse, not just in Europe.

Hence, perhaps the most speculative and important question that this essay leaves us with is the following. What might the spread of this matrix of organisational and institutional solutions - which we have characterised as alternative to the typical responses of the Fordist-Keynesian era - suggest in terms of restructuring the forms of political governance?

This question can be unpacked in two ways. The first concerns the approach to a question that is as necessary as it is widely disregarded, namely: how will public administrations be restructured by digital transformation? We noted at the outset how cloud computing brings this issue to the fore and how it touches on sensitive areas of sovereignty and power allocation, causing predictable resistance to its deployment in public administration. This matrix probably has much to say about the governance of this transformation, and at first glance, public administration offers - at least in the abstract - a prime ground for its potential exploitation. The Indian government, in fact, has taken some steps in this direction. The second way of unpacking the issue is no less difficult. In fact, it is about the political and economic macro governance of the digital transformation and the exploration of innovative political and economic solutions that fall outside the traditional state and market models.

This exploration of new institutional forms has often taken place in recent decades around what has been called the **governance of the commons** (Ostrom, 1990; Hardt & Negri, 2009). The study of the commons has expanded more and more as the digital revolution has progressed. And as we have seen, digital commons have "officially" entered in EU documents as a source of possible innovative solutions in the development and political governance of digital technologies. But the commons still remains a field of study and action in the making. The first wave of commons studies endeavoured to define the specific characteristics of the commons as an autonomous sphere distinct from the market and the state (Berlinguer, 2020a).

However, the evolution of FOSS highlights how essential it is deepen the understanding of hybrid arrangements among all these distinct institutional orders. It is from this hybridity that a new institutionalism and new forms of political and economic governance will plausibly emerge. Moreover, the size and scope of these systems, the entry of states into their governance, and the broader international context require the articulation of these innovations on a broad, systemic, political, and even global scale. With this in mind, it is certainly worth exploring how the application of new governance principles to this matrix - which has emerged from the trajectory and evolution of software systems and technologies, which was the area where the rediscovery of the commons in the digital age pragmatically began - can advance this research, the field of commons studies, and support the articulation of new policy experiments.

At the European level, as well as globally, perhaps the most crucial contribution that this matrix can make is to help imagine and experiment with new forms of collaboration.

BIBLIOGRAPHY

Amadeo, R. (2013) Google's iron grip on Android: Controlling open source by any means necessary, *Ars Technica*, 21/10/2013.

Arcesati, R. & **Meinhardt, C.** (2021). China bets on open-source technologies to boost domestic innovation. *Merics Primer*.

Arrow, K. J. (1972). *Economic welfare and the allocation of resources for invention* (219-236). Macmillan Education UK.

Arthur, W. B. (1996). Increasing returns and the new world of business. *Harvard business review, 74* (4), 100-109.

Arthur, W. B. (2009). *The nature of technology: What it is and how it evolves*. Simon and Schuster.

Arvidsson, A. & **Peitersen, N.** (2013). *The ethical economy – An Argument for the Democratization of Value*. Columbia University Press.

Baldwin, C. Y. & **Clark, K. B.** (2000). *Design rules: The power of modularity* (Vol. 1). MIT press.

Baldwin, C. Y. (2008). Where do transactions come from? Modularity, transactions, and the boundaries of firms. *Industrial and corporate change, 17* (1), 155-195.

Baldwin, C. Y., & **Henkel, J.** (2012). The impact of modularity on intellectual property and value appropriation. *Harvard Business School Finance Working Paper*, (12-040).

Baldwin, C. Y. (2018). Design Rules, Volume 2: How Technology Shapes Organizations: Chapter 14 Introducing Open Platforms and Business Ecosystems. *Harvard Business School, Harvard Business School Research Paper Series*, 19-035.

Barcevičius, E., **Cibaitė, G.**, **Codagnone, C.**, **Gineikytė, V.**, **Klimavičiūtė, L.**, **Liva, G.**, ... & **Vanini, I.** (2019). Exploring Digital Government transformation in the EU. *Publications Office of the European Union, Luxembourg*.

Barker, T. (2020). Europe Can't Win the Tech War It Just Started. *ForeignPolicy.com*

Berlinguer, M. (2023). Open Source and Economic Models in an Evolutionary Approach. In *Business Models and Strategies for Open Source Projects* (pp. 18-49). IGI Global.

Berlinguer, M. (2021). Digital Commons as new Infrastructure: A new generation of public policy for digital transformation. *Umanistica Digitale*, (11), 5-25.

Berlinguer, M. (2020a). New commons: Towards a necessary reappraisal. *Popular Communication, 18* (3), 201-215.

Berlinguer, M. (2020b). Commons, Markets and Public Policy. *Transform! ePaper*.

Berlinguer, M. (2018). The value of sharing. How commons have become part of informational capitalism and what we can learn from it. The case of FOSS. *Rassegna italiana di sociologia, 59* (2), 263-288.

Berlinguer, M. (2016). Quantifying Value in Commons-based Peer production. Paper presented at Digital Method Winter School Seminar. University of Amsterdam.

Bloomberg, J. (2018). Digitization, digitalization, and digital transformation: confuse them at your peril. Forbes. *Retrieved on August, 28*, 2019.

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, 107 (1), 1-68.

Bratton, B. H. (2016). *The stack: On software and sovereignty*. MIT press.

Brennen, J. S., & **Kreiss, D.** (2016). Digitalization. *The international encyclopedia of communication theory and philosophy*, 1-11.

Bauwens, M. (2005). The political economy of peer production. *Ctheory*. Net.

Benkler, Y. (2002). Coase's penguin, or, linux and "the nature of the firm". *Yale law journal*, 369-446.

Benkler Y. (2006). T*he Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press

Benkler, Y. (2013). Commons and Growth: The Essential Role of Open Commons in Market Economies. *University of Chicago Law Review*.

Benkler, Y. (2016). Degrees of freedom, dimensions of power. *Daedalus, 145* (1), 18-32.

Blind, K., & **Jungmittag, A.** (2008). The impact of patents and standards on macroeconomic growth: a panel approach covering four countries and 12 sectors. *Journal of Productivity Analysis, 29* (1), 51-60.

Blind, K. (2016). 14. The impact of standardisation and standards on innovation. *Handbook of innovation policy impact*, 423.

Blind, K., **Böhm, M.**, & **Thumm, N**. (2019). The Relationship Between Open Source Software and Standard Setting.

Blind, K., **Böhm, M.**, **Grzegorzewska, P.**, **Katz, A.**, **Muto, S.**, **Pätsch, S.**, & **Schubert, T.** (2021). The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy. Final Study Report. *European Commission, Brussels*.

Brynjolfsson, E., & **Saunders, A.** (2009). What the GDP gets wrong (why managers should care). *MIT Sloan Management Review, 51* (1), 95.

Burson, J. 2018. "At the Crossroads of Open Source and Open Standards". *TheNewStack.io*

Cameron, D. (2023). US Spies Are Buying Americans' Private Data. Congress Has a New Chance to Stop It. *Wired*. Jul 5, 2023.

Carlisle, K., & **Gruby, R. L.** (2019). Polycentric systems of governance: A theoretical model for the commons. *Policy Studies Journal, 47* (4), 927-952.

Castells, M. (2004). Informationalism, networks, and the network society: a theoretical blueprint. *The network society: A cross-cultural perspective*, 3-45.

Cennamo, C., **Gawer, A.**, & **Jacobides, M. G.** (2018). Towards a theory of ecosystems. *Strategic Management Journal, 39*, 2255-2276.

Chandler Jr, A. D. (1993). *The visible hand*. Harvard university press.

Coase, R. H. 1937. "The nature of the firm." *economica* 4, no. 16: 386-405.

Constantinides, P., **Henfridsson, O.**, & **Parker, G. G.** (2018). Introduction — platforms and infrastructures in the digital age. *Information Systems Research, 29* (2), 381-400.

Contreras, J. L., & **Vertinsky, L. S.** (2016). Pre-competition. *NCL Rev.*, 95, 67.

David, P. A. (2007). Path dependence, its critics and the quest for 'historical economics'. *The evolution of economic institutions: A critical reader*, 120-142.

Dosi, G. (1982). Technological paradigms and technological trajectories: a suggested interpretation of the determinants and directions of technical change. *Research policy, 11* (3), 147-162.

Edwards, P. N. (2003). Infrastructure and modernity: Force, time, and social organization in the history of sociotechnical systems. *Modernity and technology, 1*, 185-226.

Edwards, P. N. (2004). "A vast machine": standards as social technology." *Science* 304, no. 5672: 827-828.

Eghbal, N. (2016). *Roads and bridges: The unseen labor behind our digital infrastructure*. Ford Foundation.

Ethiraj, S. K., & **Levinthal, D.** (2004). Modularity and innovation in complex systems. *Management science, 50* (2), 159-173.

European Commission (2009). GDP and beyond Measuring progress in a changing world. Communication. *eur-lex.europa.eu*

European Commission (2012). Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me? Communication. *eur-lex.europa.eu*

European Commission (2013). Against lock-in: Building open ICT systems by making better use of standards in public procurRoseement. Communication. *eur-lex.europa.eu*

European Commission (2016). ICT standardisation priorities for the digital single market. Communication. *eur-lex.europa.eu*

European Commission (2021). Criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interest. Communication. *eur-lex.europa.eu*

European Council (2020) Berlin Declaration on Digital Society and Value-Based Digital Government. Declaration. *digital-strategy.ec.europa.eu*

Fadhlurrahman, R. (2023). The Chaos of Maintaining Software Dependencies and How to Tame Them. *Medium*. 18/04/2023.

Farrell, J., & **Klemperer, P.** (2007). Coordination and lock-in: Competition with switching costs and network effects. *Handbook of industrial organization, 3*, 1967-2072.

Fioramonti, L. (2013). *Gross domestic problem: The politics behind the world's most powerful number*. Bloomsbury Publishing.

Florio, M. (2021). *La privatizzazione della conoscenza. Tre proposte contro i nuovi oligopoli*. Laterza.

Fraser, N. (2017). Feminism, capitalism and the cunning of history. In *Citizenship rights* (393-413). Routledge.

Frischmann, B. M. (2012). *Infrastructure: The social value of shared resources*. Oxford University Press.

Garcia, D. L. (2018). *What's New? Standards and Innovation*.

Garud, R., **Kumaraswamy, A.**, & **Langlois, R.** (eds.). (2009). *Managing in the modular age: architectures, networks, and organizations*. John Wiley & Sons.

Gawer, A., & **Cusumano, M. A.** (2014). Industry platforms and ecosystem innovation. *Journal of product innovation management, 31* (3), 417-433.

Gawer, A. (2014). Bridging differing perspectives on technological platforms: Toward an integrative framework. *Research policy, 43* (7), 1239-1249.

Geels, F. W. (2002). Technological transitions as evolutionary reconfiguration processes: a multi-level perspective and a case-study. *Research policy, 31* (8-9), 1257-1274.

Geels, F. W., & **Schot, J.** (2007). Typology of sociotechnical transition pathways. *Research Policy, 36* (3), 399–417.

Gong, C., **Liu, J.**, **Zhang, Q.**, **Chen, H.**, & **Gong, Z.** (2010, September). The characteristics of cloud computing. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 275-279). IEEE.

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government information quarterly, 26* (1), 75-81.

Haile, N., & **Altmann, J.** (2018). Evaluating investments in portability and interoperability between software service platforms. *Future Generation Computer Systems, 78*, 224-241.

Hardin, G. (1968). The tragedy of the commons: the population problem has no technical solution; it requires a fundamental extension in morality. *Science, 162* (3859), 1243-1248.

Hardt, M., & **Negri, A.** (2009). Commonwealth. *Harvard University Press*.

Heilmann, S. (2009). Maximum tinkering under uncertainty: unorthodox lessons from China. *Modern China, 35* (4), 450-462.

Heilmann, S., & **Melton, O.** (2013). The reinvention of development planning in China, 1993–2012. *Modern China, 39* (6), 580-628.

Hughes, T. P. (1987). The evolution of large technological systems. *The social construction of technological systems: New directions in the sociology and history of technology, 82*, 51-82.

Hughes, T. P. (1993). *Networks of power: electrification in Western society, 1880-1930*. JHU press.

Hunter, P., & **Walli, S.** (2013). The rise and evolution of the open source software foundation. *IFOSS L. Rev., 5*, 31.

Huth, A., & **Cebula, J.** (2011). The basics of cloud computing. *United States Computer*, 1-4

IT-Planungsrat (2022). GRoseermany's government cloud strategy: target architecture framework. Version 2.0.1 of 10 October 2022. FITKO (Federal IT Cooperation).

Izquierdo, J. L. C., & **Cabot, J.** (2018, May). The role of foundations in open source projects. In *Proceedings of the 40th international conference on software engineering: software engineering in society* (pp. 3-12).

Izquierdo, J. L. C., & **Cabot, J.** (2020). A Survey of Software Foundations in Open Source. *arXiv preprint arXiv:2005.10063*.

Jacobides, M. G., **Cennamo, C.**, & **Gawer, A.** (2018). Towards a theory of ecosystems. *Strategic management journal, 39* (8), 2255-2276.

Jain, N., & **Choudhary, S.** (2016, March). Overview of virtualization in cloud computing. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)* (pp. 1-4). IEEE.

Jessop, B. (2015). *The state: Past, present, future*. John Wiley & Sons.

Jin, K. (2023). *The New China Playbook: Beyond Socialism and Capitalism*. Penguin.

Kades, M., & **Morton, F. S.** (2020). Interoperability as a competition remedy for digital networks. *Washington Center for Equitable Growth Working Paper Series*.

Katz, M. L., & **Shapiro, C.** (1994). Systems competition and network effects. *Journal of economic perspectives, 8* (2), 93-115.

Kawalek, P., & **Bayat, A.** (2017). Data as infrastructure. UK National Infrastructure Commission.

Kazman, R., & **Chen, H. M.** (2023). The Architecture of Complexity Revisited: Design Primitives for Ultra-Large-Scale Systems.

Kindleberger, C. P. (1983). Standards as Public, Collective and Private Goods. *Kyklos, 36* (3), 377-396.

Krazit, T. (2020) The Linux Foundation became a force in enterprise tech. Is that a problem? *Protocol*. 03/09/2020.

Kuhn, T. S. (1962). 2012. *The structure of scientific revolutions*. University of Chicago press.

Lakhani, K. R., & **Wolf, R. G.** (2003). Why hackers do what they do: Understanding motivation and effort in free/open source software projects. *Open Source Software Projects* (September 2003).

Lamanna, D. D. (2023) La capitalizzazione dei dati. *Quaderni della decrescita*, Settembre/Dicembre 2023.

Langlois, R. N., & **Savage, D. A.** (1997). Standards, modularity, and innovation: the case of medical practice. *Modularity, and Innovation: The Case of Medical Practice (July 1997)*.

Langlois, R. N. (2002). Modularity in technology and organization. *Journal of economic behavior & organization, 49* (1), 19-37.

Lapenta, F. (2021). *Our Common AI Future: A Geopolitical Analysis and Road Map for AI Driven Sustainable Development, Science and Data Diplomacy*. John Cabot University. Institute of Future and Innovation Studies.

Latour, B. 2010. *Tarde's idea of quantification*. Routledge.

Lessig, L. (2008). *Remix: Making art and commerce thrive in the hybrid economy* (p. 352). Bloomsbury Academic.

Lin, J. Y. (2011). New structural economics: A framework for rethinking development. *The World Bank Research Observer, 26* (2), 193-221.

Liu, H., & **Cargill, C. F.** (2017). *Setting standards for industry: Comparing the emerging Chinese standardization system and the current US system*. Honolulu, HI: East-West Center.

Malhotra, L., **Agarwal, D.**, & **Jaiswal, A.** (2014). Virtualization in cloud computing. J. *Inform. Tech. Softw.* Eng, 4(2), 1-3.

Manovich, L. (2005). Remixability and modularity.

March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization science, 2* (1), 71-87.

Martí, A. (2022). The birth of a geopolitical EU cloud industry – Reclaiming open source as a tool for Europe's technological sovereignty. *SovereignEdge.EU* Blog. November 29, 2022

Mayer-Schönberger, V., & **Cukier, K.** (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mazzucato, M., **Kattel, R.** & **Ryan-Collins, J.** (2021). Industrial Policy's Comeback. *Boston Review*.

Mazzucato, M., **Entsminger, J.**, & **Kattel, R.** (2021). Reshaping Platform-Driven Digital Markets. *Regulating Big Tech: Policy Responses to Digital Dominance, 17*.

Mazzucato, M. (2023). A collective response to our global challenges: a common good and *'market-shaping' approach. UCL Institute for innovation and public purpose working paper, 2*.

Milinkovich, M. (2023). "Cyber Resilience Act: Good Intentions and Unintended Consequences." In *Eclipse Foundation* Blog.

Morell, M. F., **Salcedo, J. L.**, & **Berlinguer, M.** (2016). Debate about the concept of value in Commons-Based Peer Production. In *Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings 3* (pp. 27-41). Springer International Publishing.

Northrop, L., **Feiler, P.**, **Gabriel, R. P.**, **Goodenough, J.**, **Linger, R.**, **Longstaff, T.**, ... & **Wallnau, K.** (2006). *Ultra-large-scale systems: The software challenge of the future*. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

O'Mahony, S. (2007). The governance of open source initiatives: what does it mean to be community managed?. *Journal of Management & Governance, 11* (2), 139-150.

O'Neil, M., **Cai, X.**, **Muselli, L.**, **Pailler, F.**, & **Zacchiroli, S.** (2021). *The coproduction of open source software by volunteers and big tech firms*. News Media Research Centre, University of Canberra.

Opara-Martins, J., **Sahandi, R.**, & **Tian, F.** (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing, 5*, 1-18.

Ostrom, E. (1990). Governing the commons: The evolution of institutions for collective action. *Cambridge university press*.

Ostrom, E. (2010). "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." *American Economic Review, 100* (3): 641-72.

Nelson, R. R., & **Winter, S. G.** (2002). Evolutionary theorizing in economics. *Journal of economic perspectives, 16* (2), 23-46.

North, D. C., & **North, D. C.** (1992). *Transaction costs, institutions, and economic performance* (pp. 13-15). San Francisco, CA: ICS Press.

Pannier, A. (2022) Software Power. The Economic and Geopolitical Implications of Open Source Software. Études de l'Ifri, Ifri, December 2022. Pannier, A. (2023). How Big Tech is shaping the global open source ecosystem. SovereignEdge.EU

Pao, J. (2021). China hopes to launch data as new asset class. Beijing leadership hopes data trading will propel the Fourth Industrial Revolution. AsiaTimes.com

Parker, G. G., & **Van Alstyne, M. W.** (2005). Two-sided network effects: A theory of information product design. *Management science, 51* (10), 1494-1504.

Perens, B., 2005. The emerging economic paradigm of open source. *First Monday*.

Perez, C. (2003). *Technological revolutions and financial capital*. Edward Elgar Publishing.

Perez, C. (2010). Technological revolutions and techno-economic paradigms. *Cambridge journal of economics, 34* (1), 185-202.

Perez, C. (2012). Technological revolutions and the role of government in unleashing golden ages. *Journal of Globalization Studies, 3* (2), 19-25.

Perez, C. (2013). Unleashing a golden age after the financial collapse: Drawing lessons from history. *Environmental Innovation and Societal Transitions, 6*, 9-23.

Phipps, S. (2023). The ultimate list of reactions to the Cyber Resilience Act. Opensource.org

Powell, W. W. (1990). Neither market nor hierarchy. *Sociology of organizations: structures and relationships*, 30-40.

Polanyi, K. (1957), Societies and Economic Systems, in Karl Polanyi, *The Great Transformation*, Boston, Beacon Press

Polanyi, K. (2018) [original edition: 1957]. The economy as instituted process. In *The sociology of economic life* (pp. 3-21). Routledge.

Prisecaru, P. (2019). European Political Strategy Centre: A vision about EU Industrial Policy after Siemens–Alstom Deal. *Global Economic Observer, 7* (1), 100-108.

Renda, A., **Simonelli, F.**, **Iacob, N.**, & **Campmas, A.** (2019). Evaluation study supporting the interim evaluation of the ISA² programme. CEPS Project Report. June 2019.

Rezaei, R., **Chiew, T. K.**, & **Lee, S. P.** (2014). An interoperability model for ultra large scale systems. *Advances in Engineering Software, 67*, 22-46.

Riehle, D. (2010). The economic case for open source foundations. *Computer, 43* (01), 86-90.

Rose, C. (1986). The comedy of the commons: custom, commerce, and inherently public property. *The University of Chicago Law Review, 53* (3), 711-781.

Rullani, E. (2009) I premi Nobel per l'economia, anno domini 2009. Ovvero, l'economia dei commons e delle reti, che popolano la Terra di Mezzo tra mercato e piano, Retrieved. CriticalManagement.uniud.it

Seaman, J. (2020). China and the new geopolitics of technical standardization. *Notes de l'Ifri, 34*, 20-21.

Shapiro, C., **Hal R. V.**, and **Shapiro C.** (1998). *Information rules: A strategic guide to the network economy*. Harvard Business Press.

Sharma, C. (2019). Concentrated digital markets, restrictive apis, and the fight for internet interoperability. *U. Mem. L. Rev., 50*, 441.

Sidak, J. G. (2016). The value of a standard versus the value of standardization. *Baylor L. Rev., 68*, 59.

Simon, H. A. (1962). The architecture of complexity. *Proceedings of the American philosophical society, 106* (6), 467-482.

Sommerville, I., **Cliff, D.**, **Calinescu, R.**, **Keen, J.**, **Kelly, T.**, **Kwiatkowska, M.**, ... & **Paige, R.** (2012). Large-scale complex IT systems. *Communications of the ACM, 55* (7), 71-77.

Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.

Steinmueller, W. E. (2003). *The role of technical standards in coordinating the division of labour in complex system industries* (133-151). Oxford University Press.

Sullivan J. (2023a). Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution. *WhiteHouse.gov*

Sullivan, J. (2023b), The Sources of American Power. A Foreign Policy for a Changed World, *ForeignAffairs.com* November/December 2023

Synergy Group (2022). European Cloud Providers Continue to Grow but Still Lose Market Share. *Srgresearch.com*

Synopsis (2023). Open Source Security and Risk Analysis Report. *Synopsys.com*

Terzi, A., **Singh, A.**, & **Sherwood, M.** (2022). *Industrial policy for the 21st century: lessons from the past*. Publications Office of the European Union.

Van Ark, B. (2016). The productivity paradox of the new digital economy. *International Productivity Monitor, 31*, 3-18.

Varian, H. R. (2010). Computer mediated transactions. *American Economic Review, 100* (2), 1-10.

Vrana, J., & **Singh, R.** (2021). Digitization, digitalization, and digital transformation. *Handbook of Nondestructive Evaluation 4.0*, 1-17.

Villari, M., **Fazio, M.**, **Dustdar, S.**, **Rana, O.**, & **Ranjan, R.** (2016). Osmotic computing: A new paradigm for edge/cloud integration. *IEEE Cloud Computing, 3* (6), 76-83.

Von Krogh, G., **Haefliger, S.**, **Spaeth, S.**, & **Wallin, M. W.** (2012). Carrots and rainbows: Motivation and social practice in open source software development. Mis Quarterly, 36(2), 649-676.

Weber, S. (2004). *The success of open source*. Harvard University Press.

Wegner, P. (1996). Interoperability. *ACM Computing Surveys (CSUR), 28* (1), 285-287.

Weitzman, M. L. (1998). Recombinant growth. *The Quarterly Journal of Economics, 113* (2), 331-360.

Williamson, J. (1990) What Washington Means by Policy Reform. In: Williamson, J., Ed., *Latin American Adjustment: How Much Has Happened?* Institute for International Economics, Washington, 7-20.

Williamson, O. E. (1973). Markets and hierarchies: some elementary considerations. *The American economic review, 63* (2), 316-325.

Williamson, O. E. (1979). Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics, 22*, 233–261.

Williamson, O. E. (2010). Transaction cost economics: The natural progression. *American Economic Review, 100* (3), 673-690.

World Bank (2008). The Growth Report. *WorldBank.org*

NOTES

i For instance, a recent study commissioned by the French government estimated a European market for cloud computing of € 560 billion in 2030. To get an idea of such proportions, the European car market is estimated to be worth € 419.5 billion in 2027. See presse.economie.gouv.fr
The global cloud computing market is projected to grow to $2.4 trillion USD by 2030.
See fortunebusinessinsights.com

ii See for example, Kawalek & Baya (2017).

iii Source: Fadhlurrahman, R. (2023). The Chaos of Maintaining Software Dependencies and How to Tame Them. Medium. 18/04/2023. Source: medium.com

iv See srgresearch.com

v See amchameu.eu

vi See euractiv.com

vii See ec.europa.eu

viii See gaia-x.eu

ix See www.bmwk.de

x See opennebula.io

xi See digital-strategy.ec.europa.eu

xii See digital-strategy.ec.europa.eu

xiii See digital-strategy.ec.europa.eu

xiv See health.ec.europa.eu

xv See commission.europa.eu

xvi See wikipedia.org

xvii See innovazione.gov.it

xviii See commission.europa.eu

xix See innovazione.gov.it

xx See tpi.it

xxi See agendadigitale.eu

xxii See numerique.gouv.fr

xxiii See presse.economie.gouv.fr
See also latribune.fr

xxiv See lebigdata.fr

xxv See euractiv.com

xxvi See cyber.gouv.fr

xxvii See cncf.io

xxviii The exemption that the last draft of the AI Act grants to open-source AI models in certain areas (those not classified as high-risk or prohibited), goes precisely in this direction. See reuters.com
This would be a positive discriminatory policy, justified by the greater transparency, openness to competition and democratisation of adoption and innovation that open-source solutions provide.

xxix See wikipedia.org

xxx See fossa.com

xxxi See wired.com

xxxii See ncsc.gov.uk

xxxiii See coreinfrastructure.org

xxxiv See openssf.org

xxxv See commission.europa.eu

xxxvi See sovereigntechfund.de

xxxvii See european-cyber-resilience-act.com

xxxviii See govinfo.gov

NOTES

xxxix OpenForum Europe has conducted a work of collecting and organising the FOSS ecosystem's critical observations on the CRA draft and submitted a list of amendments to EU legislators. To view this discussion on the web, visit FOSS Community Google Group.

xl See swipo.eu

xli Federated solutions, furthermore, are more appropriate both for the EU's political characteristics as a Union of states and for the technical requirements of the future Edge-Cloud-IoT infrastructure.

xlii Beginning with the adoption of Linux. Linux, in fact, did not enjoy such great success as an operating system for personal computers (where Microsoft maintained its dominance). It instead found its way as a dominant platform in other areas such as mobile devices (Android is a derivative of Linux) and in servers and Web servers. This latter is the use that started to be made of Linux, since the mid-1990s, by large organisations with supercomputing needs, such as NASA or later Google, that exploited it to build relatively inexpensive huge data centers and processing capacities. This in turn highlights a paradox. Linux, often celebrated for the democratisation it brought in software production and in a crucial layer of technological innovation, provided a potent foundation to what is the processes of "industrialisation" and "platformisation" of the Internet, and the present hugely concentrated architecture in cloud computing itself. On this, see: Berlinguer, 2018

xliii This approach has been expanded to embark the theorise that the cyclical upsurges in growth depend on periods of combinatorial innovation of interrelated new technologies.

xliv This cumulative process is also the most compelling explanation for the reversal of the dominance of proprietary software in favour of FOSS, which occurred only gradually, starting at the margins and in the most innovative areas, and then accelerating around 2010 and becoming unstoppable and irresistible since then. On this reversal of hegemony, see Commons, Markets and Public Policy, pp. 29-35 (Berlinguer, 2020b).

xlv Google's Android has been one of the first and most successful examples (Amadeo, 2013; Berlinguer, 2018).

xlvi The Indian model of digital public infrastructure (DPI) provides open-source architecture in the critical domains of digital identity, payments, banking, and health in order to guarantee "sovereignty" on personal data storage and use. See nextias.com
Access to data is granted via anonymised and encrypted technologies to private businesses with consent from users using a techno-legal approach: the Data Empowerment and Protection Architecture (DEPA). See niti.gov.in

xlvii Strategies include designing for resilience and maintaining pluralism and redundancy of choices (Benkler, 2016).

xlviii There is a vast literature on this subject. See for example, Lakhani & Wolf (2003) and Von Krogh & al. (2012).

xlix The practice of "pre-competitive collaboration" in R&D has gained traction in many sectors, not just in software. See Contreras & Vertinsky, 2016.

l Many examples in different fields could be cited. Right now a notable case is provided in microchip design, by RISC-V, an open-standard instruction set architecture (ISA), which is gaining momentum, especially with the support of Chinese companies, after the introduction of restrictions on the export of advanced microchip technology to China. See https://riscv.org/. But another critical case is likely to be provided by data. See in this regard Box 10.

li There have been numerous FOSS policy failures in the past. See Berlinguer, 2020b.

lii See the Declaration by the Presidency of the Council of the European Union calling for a European Initiative for Digital Commons at: diplomatie.gouv.fr

liii See businesstoday.in and itu.int

NOTES

liv For example, several US lawmakers have shown a clear concern for the open source Risc-V project in microchip design and the intention of prohibiting American developers to participate in it.
See thehill.com
Risc-V foundations has moved from USA to Switzerand precisely to avoid to be dragged into these geopolitical clashes. See for example nasdaq.com
"I fear that our export-control laws are not equipped to deal with the challenge of open-source software - whether in advanced semiconductor designs like RISC-V or in the area of AI - and a dramatic paradigm shift is needed,"; "U.S. persons should not be supporting a PRC tech transfer strategy that serves to degrade U.S. export control laws." said US lawmakers. However, things can go in the opposite direction, in other cases. In the case of 5G, where the technological advantage is Chinese, US industry and government sponsor an open source solution: 5G open RAN.

lv In 2021, the Ministry of Industry and Information Technology's development planning guidance prominently featured open source. See interconnected.blog

lvi See techcrunch.com

lvii See gizchina.com

lviii See for example the Open Network for Digital Commerce.

lix See thehill.com

lx See nasdaq.com

lxi See reuters.com

lxii See calcalistech.com

lxiii See businessinsider.com

Members and Observers

Austria
transform! At
www.transform.or.at
Institute of Intercultural Research and Cooperation – IIRC*
www.latautonomy.com

Cyprus
Research Institute PROMITHEAS*
www.inep.org.cy

Czechia
Institut of the Czech Left (Institut české levice)*
www.institutcl.cz
Society for European Dialogue – SPED
e-mail: malek_j@cbox.cz

Denmark
transform!danmark
www.transformdanmark.dk

Finland
Left Forum
www.vasemmistofoorumi.fi
Democratic Civic Association – DSL
www.desili.fi

France
Espaces Marx
www.espaces-marx.fr
Foundation Copernic*
www.fondation-copernic.org
Foundation Gabriel Péri*
www.gabrielperi.fr
Institut La Boétie*
www.institutlaboetie.fr

Germany
Journal Sozialismus
www.sozialismus.de
Rosa Luxemburg Foundation – RLF
www.rosalux.de
Institute for Social, Ecological and Economic Studies – ISW
www.isw-muenchen.de

Greece
Contemporary Social History Archives – ASKI*
www.askiweb.eu
Nicos Poulantzas Institute – NPI
www.poulantzas.gr

Hungary
transform! Hungary*
www.balmix.hu

Italy
transform! Italia
www.transform-italia.it
Cultural Association Punto Rosso (Associazione Culturale Punto Rosso)
www.puntorosso.it
Fondazione Claudio Sabattini*
www.fondazionesabattini.it

Lithuania
DEMOS. Institute of Critical Thought*
e-mail: demos@inbox.lt

Luxembourg
transform! Luxembourg*
www.transform.lu

Moldova
transform! Moldova*
e-mail: transformoldova@gmail.com

Norway
Manifesto Foundation*
www.manifestanalyse.no

Poland
Foundation Forward / Naprzód
www.fundacja-naprzod.pl

Portugal
CUL:TRA Cultures of Labour and Socialism
e-mail: info@cultra.pt

Romania
Association for the Development of the Romanian Social Forum*
e-mail: pedroxma@yahoo.com

Serbia
Centre for Politics of Emancipation – CPE*
www.pe.org.rs

Slovenia
Institute for Labour Studies – IDS*
www.delavske-studije.si

Spain
Alternative Foundation (Catalonia)
www.fundacioalternativa.cat
Europe of Citizens Foundation – FEC
www.lafec.org
Foundation for Marxist Studies – FIM
www.fim.org.es
Instituto 25M*
www.instituto25m.info
Iratzar Foundation (Basque Country)*
www.iratzar.eus

Sweden
Centre for Marxist Social Studies
www.cmsmarx.org

Turkey
Social Investigations and Cultural Development Foundation – TAKSAV*
www.taksav.org
Sol-Blog*
https://solparti.org

UK
The World Transformed – TWT*
www.theworldtransformed.org
Transform! UK A Journal of the Radical Left
www.prruk.org

*Observers

European network for alternative thinking and political dialogue

transform! europe is a network of 40 European organisations from 23 countries, active in the field of political education and critical scientific analysis, and is the recognised political foundation corresponding to the Party of the European Left (EL).

On the transform! europe website, you can find reports on current events relevant to Europe, as well as analyses of economic, political and social topics. In order to enable direct exchange between politicians, academics and activists involved in social movements, our calendar provides an overview of relevant international conferences and events. Moreover, transform! europe enables free access to publications released or supported by the transform! network which cover a wide range of topics on a high level. They can be downloaded from the website for free.

transform! europe

www.transform-network.net