ASTRID

ASTRID PAPER

80

The cloud industry and the role of Italy in the Gaia-X project

edited by Maurizio Dècina, Alfonso Fuggetta e Antonio Perrucci

The paper is the result of the work of a study and research group set up within the Astrid Digital Ecosystem Laboratory, directed by Antonio Perrucci. The research was coordinated by Maurizio Dècina, Alfonso Fuggetta and Antonio Perrucci. Other participants in the work of the group were: Daniele Ali (Fincantieri), Franco Bassanini, Francesco Bonfiglio, Carlo Bozzoli (Enel), Luca Cardone (Retelit), Pier Luigi Dal Pino (Microsoft), Claudio Farina (Snam), Valerio Francola, Giuseppe Italiano, Paolo Lupi, Dario Pagani (Eni), Franco Pizzetti, Federico Protto (Retelit), Franco Spicciariello (Amazon Web Services), Giorgio Veronesi (Snam). Amazon Web Service, Enel, Eni, Fincantieri, Microsoft and Snam contributed to the funding of the research.

The first version of the paper, in Italian, was published in May 2021. This new version, in English, edited by Gordon A. Mensah, has been revised and updated with the contribution of Francesco Bonfiglio, Alfonso Fuggetta, Antonio Perrucci and Valerio Francola.

However, the responsibility for what is claimed in the paper lies exclusively with Astrid and the editors who wrote it.

DECEMBER 2021

The research project benefited from the collaboration as sponsors of:

aws

enel

eni

FINCANTIERI
The sea ahead

Microsoft

snam

Index

Executive Summary

Introduction

Chapter 1. The cloud industry: infrastructure, market and "technical" regulation aspects

1.1. Cloud Computing and Gaia-X

1.2. Outline of the technical aspects of Cloud Computing systems

1.3. The service models

1.4. Cloud deployment models

1.5. Data Security and Resilience in the Cloud System

Chapter 2. The "legal-economic" regulation of the cloud: the issue of data

2.1. The "traditional" approach to market regulation

2.2. The regulation of digital services and markets

Chapter 3. The competitive structure of the European cloud market: possible evolutions

3.1. A general framework

3.2. The determinants of enterprise uptake of cloud services

3.3. The cloud for Public Administration: insights for the Italian experience

3.3.1. The history of information technology in PA: an outline

3.3.2. The rationalization of the IT services of Public Administrations

3.3.3. Italian National Cloud Strategy

Chapter 4. First conclusive considerations

4.1. Setting an industrial strategy for the European cloud: beyond the "European cloud champion"

4.2. The nature and role of Gaia-X

Executive Summary

The idea of promoting a study group on the theme of the cloud industry - with specific reference to the Italian market - was conceived at the end of last summer, when the initiative called Gaia-X also attracted the attention of the media and they began to discuss the possible reflections for the Italian cloud. After a couple of brainstorming meetings, a working group was set up, formed mainly by managers of companies that provide and use cloud services, as well as experts with different backgrounds (technical, economic, legal). After a number of seminars in which previous versions were discussed, this text was prepared as a basis for discussion both within Astrid and with external interlocutors, i.e. industry representatives and policy makers. At the end of these in-depth discussions, it will be possible to revise this report, also integrating the analysis with other components that it was not possible to examine on this occasion, such as, for example, the theme of digital skills.

The document is structured in four sections. The first - by way of introduction - describes the profiles of technical and infrastructural nature, the characteristics of the offer and the service models, the problems related to security, with some hints at the so-called "technical regulation" of the cloud. The second section is an in-depth analysis of regulatory aspects, with attention to both the cloud market and the data market, the latter being the subject of various interventions by the European Commission. In the third section, the market structure of the cloud industry is analyzed, evaluating the possible development trajectories, also in the light of the Gaia-X project. In this context, a particular attention is reserved to the cloud of the Public Administration. The last section, finally, proposes some conclusive considerations that are summarized below.

Basically, there were four major themes, or rather questions, that occupied the working group, which, in the end, arrived at as many answers, in some cases proposing more than one alternative.

The first question concerned the theme of the "European champion" of the cloud: a theme that has never been explicitly represented in the work of Gaia-X, especially in the initial phase, but also now in the current configuration of the European Association. In turn, this "dilemma" leads to the question of where the Gaia-X project stands among the various models it might refer to (discussed below).

The prospect of a European champion in the cloud market, challenging the big U.S. and Chinese players, never evoked by Gaia-X, is instead a stated goal of Commissioner Breton, in speeches at workshops and conferences, especially as part of the (little known) activities of the European Alliance on Industrial Data and Cloud (AIDC, also Alliance[1]).

[1] For what concerns the recent developments of the Alliance please refer to https://digital-

In this regard, it remains to be better understood what the relationships between the activities of the two initiatives are: Gaia-X and the mentioned Alliance. On this - crucial - step, we expect an important contribution from the discussion occasions of the paper presented here. In particular, we believe that that certain initial ambiguity in the Gaia-X project in relation to extra-regulatory profiles will be progressively resolved with the Association's own operativeness, as well as when the relationships with the Breton Alliance become clearer. With reference to the current situation, and based on previous experiences, the conclusion of the working group regarding the promotion of a European cloud champion is clear: for various reasons, the hypothesis of constituting a European champion able to challenge the large American and Chinese operators appears unrealistic.

In the opposite direction to such a hypothesis, it is first of all recalled the 10-15 years delay that the European cloud industry has with respect to international competitors: a delay that seems unbridgeable, especially for the rhythm that technological innovation continues to develop in this sector. A deterrent to move in this direction also comes from the experience of those countries (France) that have tried - without success - to build a "national champion" of the cloud industry. Then there are the competition concerns which - plausibly - could be raised by the antitrust authorities, at a community and/or national level, for the establishment of an entity capable of reducing the degree of competition, above all at the level of a single national market. Lastly, there is a "political" perplexity regarding the "nationality" of the European sample which, in fact, would risk being the re-proposition of a national sample, this time on a European scale. In any case, the working group is not prejudicially opposed to the idea that public intervention in support of the cloud and data industry, in certain circumstances, can also take the form of support for private investment, possibly through forms of public/private partnership. This brings us to a second issue, which concerns our country more closely, because it represents a project of the previous Minister for Technological Innovation and Digital: the establishment of a public/private joint venture for the provision of cloud services to the Public Administration. In particular, to a significant number of large central public administrations. This is a project that raises a lot of concerns among the participants in the working group, who do not understand its motivations, at least from what we have been able to learn about the contents of the initiative. In this regard, in addition to observing that there is already a "specialized" cloud service provider for the PA (Sogei for the requirements of the Ministry of Economy and Finance), it is believed that this fragmentation of the public demand for cloud services is not economically meaningful, while at the same time it would amplify the problems of interoperability of systems.

Moreover, beyond the declarations regarding the freedom of public administrations to freely choose their own supplier on the market, and therefore also a party other than the joint venture, it appears evident that the prospects for success of this new public/private operator - if any - are linked to the potential of having a captive clientele, represented precisely by the large central administrations. The Government, promoter of the joint venture, would therefore be

strategy.ec.europa.eu/en/library/today-commission-receives-industry-technology-roadmap-cloud-and-edge induced to exercise moral suasion on the central administrations, which would - in fact - restrict their freedom of choice and, certainly, would also be a guideline for other state administrations.

Should the Government decide to go in this direction and set up an Italian operator specialized in the provision of cloud services to central PA, the third issue highlighted by the working group concerns the tender conditions for the selection of the private partner (better if more than one). The recommendation of the working group is that the tender to select the partners should take place in compliance with the rules protecting competition: there can be no exclusion of participants on the basis of their nationality, size, business model or other characteristics, while it is entirely appropriate that standards of performance, security, interoperability and environmental protection in line with European principles and experience are guaranteed. Generally speaking, EU cloud and data industry regulations will also have to be applied to the possible new entity, taking into account the regulatory proposals currently under discussion (Digital Services Act, Digital Markets Act, Data Governance Act), as well as the framework of rules that will be defined by Gaia-X.

The nature, purpose and prospects of Gaia-X, now that it has become a French-European project, constitutes the fourth topic addressed by the study group. In this regard, three possible reference models have been envisaged: a GSM like model, aimed at the definition of "technical" rules (privacy, security, inter-operability, environmental protection); an Airbus like model, which foresees an industrial intervention, in the form of direct public investments; a "third way", defined as "hybrid", in which - in addition to the rules - a function of standardization and brokerage towards market services is also envisaged. However, examining the most recent work of the Association, a fourth possible scenario was highlighted, which could be considered a different version of the "hybrid" model. In fact, it was observed that - alongside the "prevailing" mandate to deal with the framework of rules and standards - there is also an emerging intervention to promote a logical layer placed on top of existing cloud infrastructures. As can be inferred from the positions expressed by authoritative representatives of the Association, in addition to the definition of the rules, the Gaia-X project should also deal with an industrial profile: that is, the elaboration of software components that will have to be adopted and implemented by anyone wishing to offer services conforming to the model proposed within the Gaia-X initiative.

In order to stimulate an open and non-ideological debate among policy makers and operators in the sector, the working group presents all three hypotheses, but, at the same time, declares the almost unanimous preference of its participants for the GSM like option - possibly integrated with coordination functions - and the deep distrust for an Airbus like solution.

Finally, as a general recommendation, the working group invites to take into account the experiences gained in the past, both in other countries (experience of the French "national champion" of the cloud) and in our country.

In particular, in the context of the cloud strategy that the new Minister for Innovation and Digital Transition will have to define, it becomes fundamental to also take into account the synergy between the enabling structure and the role of the Public Administration in digitalization processes, as will be indicated in the PNRR (National Recovery and Resilience Plan).

In this regard, it must be remembered how government intervention, both at central and local level, has often been centered, even recently, on the new technologies to be adopted and on the development and provision of front-end services (portals, apps, payment systems, digital identity) and not also on the theme of reengineering and revision of PA processes and products[2].

A change of perspective of this kind would create the conditions to finally make possible a direct communication between administrations and, from the IT point of view, the full interoperability of the back-end, the consolidation of the country's databases the rationalization of the applications park, a prerequisite for the transition to the cloud and the optimization of data centers and processing systems of the administrations.

From this point of view, as already mentioned above, the public sector should increasingly focus on the management of the country's strategic assets (databases and back-end systems), leaving room for the private sector to provide front-end services. In the - very peculiar - circumstances in which, on the other hand, the State decides to operate in the market with its own offer, it will inevitably have to deal with market conditions, in compliance with current regulations and antitrust rules.

[2] These themes (in particular the distinction between front-end and back-end and the need to make PA back-ends interoperate in order to develop really useful front-ends) were already present in the Action Plan for e-government elaborated in 1999 by Prof. Alessandro Osnaghi on behalf of the Minister for Public Administration Franco Bassanini and presented in 2000.

Introduction

The Gaia-X initiative, promoted by the Governments of France and Germany in June 2020, with the initial participation of 22 companies from the two countries (11 from Germany and 11 from France), took on a more robust dimension in September 2020 with the establishment by the founding members of an international non-profit association under Belgian law, Gaia-X AISBL [3](from French: *association internationale sans but lucratif*).

Of significant importance is the support to the initiative that came from the Joint Declaration of 25 member countries in October 2020[4]. In this way, the initiative has taken on a European and at the same time institutional dimension.

In the meantime, Gaia-X AISBL has progressively gained the adherence of companies and institutions from other European countries, registering several hundred partnership requests.

In this context, Italy - i.e. individual companies and some industry associations - have displayed great interest, applying to play a leading role.

To do what? This question may seem superfluous, in light of the programmatic documents of the Gaia-X Association, available on its website.

Instead, in our opinion, at least in the initial phase and in a more attenuated way still today, there has been a basic ambiguity on what the objectives of the initiative are. These can be simplified by indicating two paths.

The first, of a regulatory nature, concerns the definition of a framework of rules - technical and "legal" - to ensure that the provision of cloud services, by any provider, takes place in compliance with European standards on privacy, personal data protection, security, environmental protection. In short, Europe promoting adequate regulation, both of a technical nature, with regard to standards, as happened for GSM in the case of mobile telephony, and of a "legal-economic" nature. Under this last profile, the most recent examples concern: the General Data Protection Regulation (2016), the regulation of online copyright (2019), the Directives on the regulation of electronic communications and audio-visual services (2018) and the recent package of regulatory proposals on data and platforms (end of 2020; see below, paragraph 2.2) and Artificial Intelligence (April 2021).

[3] For what concerns the recent developments of Gaia X Association please refer to: https://www.politico.eu/article/gaia-x-ceo-francesco-bonfiglio-european-cloud-project-france-exit/

[4] Joint declaration, Building the next generation cloud for business and the public sector in the EU, 15 October 2020.

In this regard, the expression "Brussels effect" has been coined to indicate Europe's ability to establish a framework of rules that becomes a reference for other countries, first and foremost Western ones[5].

The second path is instead less evident, never explicitly indicated, at least in the context of Gaia-X works: the idea of constituting a European champion in the cloud market, in order to contrast the undoubted hegemony of the big US operators (Amazon, Microsoft, Google, first of all) and the advent of the Chinese ones (Alibaba).

In this case, the "Airbus model" has been evoked, i.e. a challenge brought to the industrial level, in order to juxtapose it with the "GSM model" or - more generally - the strategy based on the definition of rules consistent with the respect of the fundamental values on which the European Union is based.

In this policy brief, we will examine both perspectives, and some possible alternatives.

Chapters 1 and 2 are devoted to examining regulation.

In detail, the first chapter recalls some technical aspects of Cloud Computing systems, illustrates the main services and cloud models currently available on the market, and mentions the security profiles.

The second chapter, deals with the "legal-economic" regulation, with specific attention to the discipline of data, a topic related but distinct from that of the cloud industry: ownership and access, are essentially the aspects considered. In particular, will be examined the possible paths for a discipline of data and cloud services within the instrumentation available to the European Union.

Chapter 3 will be dedicated to examining the competitive and industrial implications, with an analysis of the "industrial policy" initiatives underway or announced by the European Union. Specific attention will be given to the project of a national cloud for the Public Administration, as initially foreseen by the Simplification Decree[6] and now included among the projects of the National Plan for Recovery and Resilience (PNRR) presented by the Government.

Finally, in chapter 4, we will make some concluding remarks, at the state of knowledge and debate, both in strong evolution, with regard to the prospects of a "European champion" able to compete with companies that dominate the global cloud industry, and what possibilities there are to strengthen the bargaining power of customers, that is, companies and public administrations that, increasingly, are oriented towards cloud

[5] Anu Bradford, The Brussels Effect: How the European Union Rules the World, Oxford University Press, 2020.

[6] The decree includes provisions aimed at encouraging the creation of a national cloud to protect the technological autonomy of the country, secure the digital infrastructure of the Public Administration, ensure the quality and security of data and digital services.

services, giving up to internalize activities of collection, storage, processing of their data.

Some first reflections will be devoted to examining the different possible perspectives of the Gaia-X project, in order to acquire points of view of the research partners, for a subsequent elaboration, in the light of the mentioned evolutions of both Gaia-X and the Alliance on Cloud and Data.

Chapter 1.
The cloud industry: infrastructure, market and "technical" regulation aspects

1.1. Cloud Computing and Gaia-X

Cloud Computing is an IT paradigm thanks to which it is possible to offer remote access to hardware and software resources according to a variety of means and options aimed at satisfying a plurality of needs by leveraging the virtualization and efficient orchestration of usable resources, also in shared mode, but with adequate guarantees of security, privacy and data sharing[7].

Cloud Computing offerings are broken down by service models (*infrastructure, platform and application*) and deployment models (*public, private, community and hybrid*). More recently, as the location of processing resources has become particularly important, a distinction has also begun to be made between Core Cloud and Edge Cloud. In particular, the Core Cloud centralizes computational resources in large data centers, to ensure high performance in data processing and storage, while the Edge Cloud distributes resources in data centers located close to users, to ensure low latencies in the transmission of critical information and improve the delivery of large volumes of traffic (resulting in reduced network traffic).

Core Cloud services are mainly offered by the large multinational Over The Top (OTT) players, which in this context are also called *Hyperscalers* (Amazon, Microsoft, Google, etc.), while *Edge Cloud* services are within the reach of the operators present in the territories where the users are located and that can enhance their assets to host *mini-datacenters*.

The European federated cloud ecosystem Gaia-X, on the other hand, through the definition of open and shared interfaces between players, allows the creation of a flexible model that provides the market with the possibility of:

1. accessing a variety of alternative offerings and managing provider switching and data portability with marginal impacts;
2. benefit from a European supervision for the compliance with the requirements and standards of security, privacy and ownership in the processing of data;

[7] It is important to clarify in this context the difference between cloud infrastructure and application: the cloud can be defined as a "container" within which data is placed but without allowing the owner of the cloud infrastructure to have access to that data. The cloud does not manage the data, it hosts applications that are the entity that has access to the data. These are therefore two distinct markets.

3. build in a simplified way hybrid private and public multi-cloud strategies, with appropriate calibration between *Edge and Core Clouds.*

The federated approach has the advantage of allowing the growth of the entire ecosystem in an open way, going to enhance in a virtuous way the specific assets of the operators present in the territory and those of the big international players.

It is essential to underline that the transformation process enabled by the cloud in its most modern and complete formulation is not a mere transfer of processing stacks from the computer room, or from the company's data center to Cloud systems (according to what is called "lift & shift") but involves a real revision of internal and external processes of organizations, with a radical reconfiguration of operating modes, value chains and often business models.

The development of a clear strategic reference framework and the maturation at companies of a culture and skills able to deeply grasp the cues of digital transformation are a key factor for the development of the country's economy.

1.2. Outline of the technical aspects of Cloud Computing systems

In general, there are three technologies at the base of Cloud Computing: virtualization, multitenancy mechanisms and service-oriented architectures (SOA - Service Oriented Architecture).

The essential technological component is virtualization, i.e. the possibility of associating the physical part of the infrastructure with a virtual computing environment or other applications (e.g. storage). Virtualization consists in creating virtual versions of physical resources, such as servers, memory space and network systems, as in the case of the Infrastructure as a Service model, which will be discussed below.

Virtualization allows you to dynamically define the characteristics of virtual resources and their mapping to real resources. This allows for resource optimization and the ability to cope with changes in user usage requirements.

The second component is multitenancy. This term refers to an architectural principle whereby a single instance of an application installed on a machine (the Cloud Provider's) can be used by multiple users (the clients of the Cloud service), while keeping the data separate. It is therefore possible to activate a single instance of the service (i.e. the software application) without having to replicate dedicated isolated architectures.

Service-oriented architecture refers to a set of architectural design principles that enable the integration and addition of services, without redesigning the internal software architecture. The operation is given by the interaction of different services, each of which performs a micro-function (microservices).

Through an SOA architecture it is possible to add new services or update and modify the way in which services are delivered or interact with each other, to better respond to specific needs.

This is very useful in cloud computing architectures, where you can "turn on" or "turn off" services relatively easily as needed."

1.3. The service models

The National Institute of Standards and Technology (NIST), defines three service models for Cloud Computing. These are three models that represent three different alternatives offered to customers, in which the responsibility between customer and service provider is modulated differently, and therefore the delegation to the service provider of service provider to carry out tasks of procurement and operational management of hardware and software resources that make up the infrastructure of delivery of cloud services.

All service models and all vendors offer portal-based service configuration, purchasing and provisioning interfaces with graphical user interfaces and guides that enable customers to purchase and pay for services online, as well as perform operational management and performance monitoring (self-service mode).

The Infrastructure as a Service (IaaS) model envisages that the client is supplied with basic infrastructure services such as processing facilities (cores equipped with resources taken from a catalog of alternatives) and mass storage (also in this case with characteristics and dimensions from a catalog). Normally, the purchase of these components is accompanied by the purchase of services related to the network, useful both for the realization of connections between the components in the cloud, but also for communication between the data center and the customer's sites.

The Platform as a Service (PaaS) service model requires the customer to obtain from the supplier services with higher added value than processing and storage infrastructures, and more precisely development environments or middleware tools (e.g. databases, ERP, CRM, Portals, ...), on which to base the development of their own applications, configuring the platforms or developing parts of their own code. In this case the frontier of responsibility moves further towards the supplier, with advantages that are added to those already highlighted for the IaaS model, further reducing the system load and the burden of supplying on their own (as an investment) of development platforms and middleware. In the area of the PaaS model, which is aimed at developers and therefore not at the end users of an application service, the development paradigm (called Cloud Native) of Container as a Service (CaaS) and Function as a Service (FaaS), which offer greater flexibility in the modularization of the functional components involved, can also be traced back.

The Software as a Service (SaaS) model completely outsources the IT stack, with the customer procuring an application service, typically standard, offered by the provider, further shifting the line of responsibility to the provider and extending the benefits to the application area as well, completely eliminating the burden of programming and system management and making application services directly available to end users.

The term Everything as a Service (XaaS) encompasses the wide range of products, tools and technologies that are emerging as new and popular cloud service offerings. of cloud services, each focused on one area and for which a specific term has been coined.

Some of the most well-known services include Desktop as a Service (DaaS), Disaster Recovery as a Service (DRaaS), Unified Communications as a Service (UaaS), Artificial Intelligence as a Service (AIaaS), Blockchain as a Service (BaaS) and CRypto as a Service (CRaaS), and so on.

1.4. Cloud deployment models

Along with service models, NIST defines four deployment models for cloud computing technologies: public, private, community, and hybrid.

The public cloud model involves the provision of public computing services over the Internet by a provider that invests in computing resources and places them in its own distributed data centers.[8] Public cloud services are offered to the market, either for a usage-based fee, or (even) for free. In the public cloud, the provider is responsible for managing and maintaining the systems and the physical environment in which they are securely deployed.

The private cloud model involves providing IT resources and services to a single organization that accesses them via the Internet or a private internal network. A private cloud can be managed internally by the organization, which has its own infrastructure and operating facilities, or by a third-party vendor to which it outsources service delivery, which can have various degrees. The private cloud offers many of the benefits

[8] Public cloud services can also be delivered via private connections and not over the public internet. What is relevant to the definition of public cloud is that cloud infrastructures are not dedicated to a single customer, but shared among multiple customers and therefore, as such, "public".

of the public cloud, including self-service and scalability, but it also allows for greater control of resources and data and greater customization of services. These prerogatives are tied to the goal of directly implementing and governing levels of security and privacy.

The community cloud, or Community Cloud, is a deployment model based on an infrastructure shared by several organizations that have agreed to a form of sharing between known parties (who make-up the Community) with the goal of achieving a restricted and more controlled form of sharing.

A hybrid cloud is realized when IT services are organized by combining public and private cloud implementations, with a workload distribution that maps the two modalities in a targeted way in relation to the requirements/cost balance of the different automation domains.

In this scenario, which is extremely common and is in any case present during the gradual adoption of the cloud, appropriate mechanisms must be put in place to manage the partitions of systems in the two areas and any relationships or needs for inter-work.

The concept of multi-cloud, i.e. the use by a single organization of the services of multiple cloud providers, is a concept that is spreading rapidly in the market with the dual purpose of adopting the solutions proposed by different service providers that best meet its needs and reducing dependence on a single provider. Clearly, the multi-cloud option can be combined with hybrid modes (resulting in a "hybrid multi-cloud" arrangement).

As the number and size of IT workloads continues to grow, so too does the market's need for the most flexible cloud structure possible to accommodate established workloads and native cloud applications. Thus, a multi-cloud approach may be the most suitable strategy for this type of need. Gartner predicted that by 2020, 75% of companies using IaaS services on cloud infrastructure will adopt a multi-cloud strategy. A prediction that, according to reports from Flexera, which will be discussed below, turned out to be correct.

The term multi-cloud in recent years has had two meanings. The first one is related to users who use different Cloud infrastructures both for the IaaS part and for the PaaS and SaaS parts: these are typically companies that use a cloud provider for the purely infrastructural part of their IT platforms and that use SaaS or PaaS solutions for some types of business software (for example online CRM such as Salesforce, Dynamics 365, online ERP or collaboration tools such as Office 365 or Google Suite). The second meaning is instead related to the need to expand the theme of hybrid cloud infrastructure across multiple public cloud providers. This is the multi-cloud infrastructure model that should allow companies to take advantage of the IaaS part on multiple cloud platforms, both private and public, also integrating Edge computing resources. A typical example is a company that wants to use virtual machines or containers on multiple platforms, selecting the solutions that best suit its needs in terms of both performance and economic efficiency from a single cloud provider.[9] All orchestrated by a single delivery platform. Looking at the multi-cloud infrastructure market, there are still few solutions that can handle these levels of complexity.

The first Hyperscaler to jump on this type of service is Google Cloud with Anthos just under two years ago.

In fact, the Anthos platform is capable of managing multiple types of workloads, in multiple environments (Amazon's AWS, Microsoft's Azure, and Alphabet's Google Cloud), in multiple locations (regions)[10].

The second case is what Microsoft is proposing with Azure, Arc. Through a single control panel, customers can manage Azure resources across multiple clouds. This means that all Azure innovations are technically available anywhere, regardless of whether they are on cloud or even on-premises.[11]

Also, AWS with the Outposts platform responds to the needs of customers who want to take advantage of hybrid cloud architectures. The service allows customers to use AWS computing and storage services such as Virtual Machine and Storage within their own data centers, but with hardware provided by AWS in combination with public cloud resources.

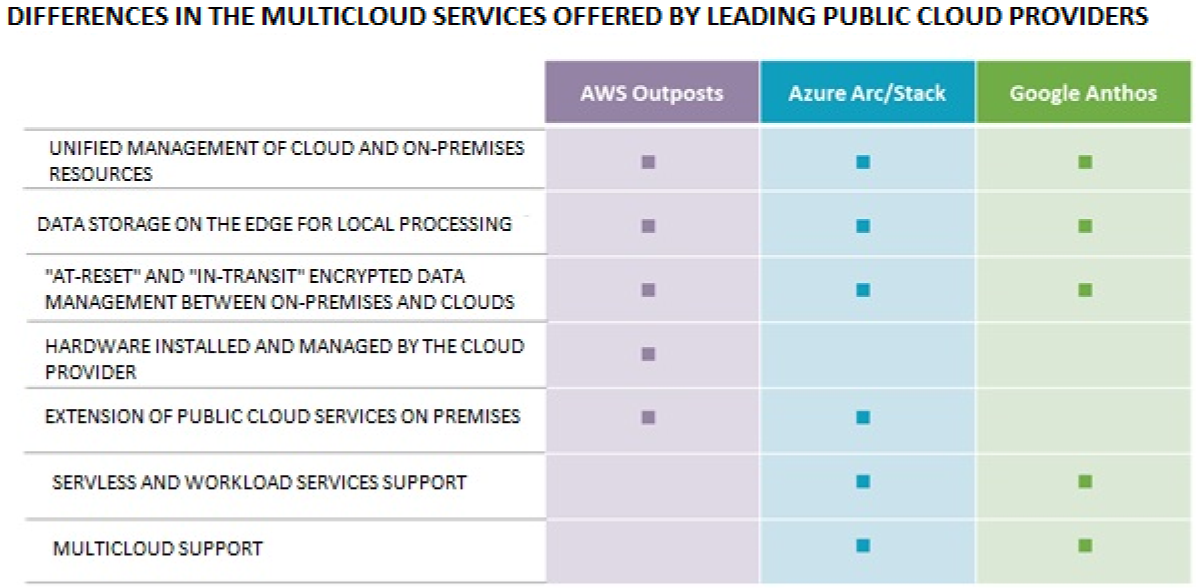
Google Cloud, Anthos, and Microsoft Azure Arc have fairly similar technical approaches; both leverage Kubernetes and containers to provide complete solutions: on-premise, in their own public cloud platform, or in a competitor's cloud.

AWS Outposts, on the other hand, focuses exclusively on customers who need to have on-premise solutions combined with public AWS resources. Moreover, by using hardware provided by AWS itself, Outposts tends to simplify the hybrid model and safeguard the customer's investment by using its own hardware engineered to best support AWS cloud software.

[9] Using Amazon's S3 for example by combining the ECS part - virtual machines - across multiple clouds such as those in Azure and AWS itself.

[10] Anthos' solution is particularly focused on containerization solutions using Kubernetes. In fact, Anthos enables organizations to run Kubernetes on both cloud and on-premise, providing simplified management in terms of installation, upgrade, configuration management, security and observability.

[11] Arc also supports Kubernetes VMs and clusters running on other public clouds like AWS and Google Cloud.



DIFFERENCES IN THE MULTICLOUD SERVICES OFFERED BY LEADING PUBLIC CLOUD PROVIDERS

	AWS Outposts	Azure Arc/Stack	Google Anthos
UNIFIED MANAGEMENT OF CLOUD AND ON-PREMISES RESOURCES	■	■	■
DATA STORAGE ON THE EDGE FOR LOCAL PROCESSING	■	■	■
"AT-RESET" AND "IN-TRANSIT" ENCRYPTED DATA MANAGEMENT BETWEEN ON-PREMISES AND CLOUDS	■	■	■
HARDWARE INSTALLED AND MANAGED BY THE CLOUD PROVIDER	■		
EXTENSION OF PUBLIC CLOUD SERVICES ON PREMISES	■	■	
SERVLESS AND WORKLOAD SERVICES SUPPORT		■	■
MULTICLOUD SUPPORT		■	■

There are also some national cloud providers that are developing through proprietary orchestrators and use of open-source platforms such as Openstack this kind of functionality. For example, in Italy, Retelit, proposes itself as a multi-cloud operator able to orchestrate IaaS platforms on multiple cloud environments both private and Azure and AWS.

There are also private realities that are starting to adopt similar solutions by relying on vendors that offer commercial solutions able to guarantee multi-cloud in typically containerized environments.

Some of the products that might fall into this category include.

- VMware CloudHealth / Tanzu
- Giantswarm
- Rancher
- Embotici
- Flexera

These platforms, in particular, deal with provisioning, automation, cost optimization, policy governance and cost control.

A further push on multi-cloud comes from Gaming companies that through the use of containers and data centers geographically distributed on the territory in Edge computing mode are interested in using the multi-cloud mode to make available containers on different platforms, but close to the end user and therefore able to ensure the best user experience and low latency.

Recently, there has been a growing interest in Edge Computing, which is the trend towards services that make use of resources, such as processing or storage capacity, deployed close to the places where data is generated and used.[12] The term Edge, to indicate the edge or periphery of the network, contrasts with Core, which involves the localization of IT resources in remote data centers, often with undefined and changing geographic locations.

A shift from the center to the periphery, from the core to the edge, which represents a paradigm shift especially for cloud-native applications. The edge computing model doesn't just want to "move" the problem from the core to the periphery, but to make network and data management smarter. The application, therefore, can be developed to manage data that needs little processing on the peripheral nodes and instead send those that need high processing capabilities to the central system.

It is precisely on the concept of proximity that edge computing is founded. It works by moving data storage, management and processing to edge nodes, where data is generated by applications, devices and users, away from the centralized cloud or central network. Edge nodes can take the form of small data centers, micro-data centers in shelters as well as individual devices or sensors.

Edge computing can be advantageously applied wherever bandwidth, low latency or localized management of large volumes of data are crucial and critical to the delivery of high-quality services.

In the area of content delivery and network optimization we see how the application of solutions such as Content/DNS Caching at the edge actually improves the user experience ("QoE Improving") of the customer and optimizes transport costs and data traffic management in operators. Performance Optimization solutions such as Protocol Accelerators and breakout sessions, on the other hand, are able to optimize the TCP application flow by intercepting the call on the edge in order to decrease the delay due to the higher latency towards the core.

With the advent of IoT and 5G, operators are adopting Multi-access Edge Computing (MEC) solutions to implement Cloud-Radio Access Network (Cloud-RAN) functions to modernize the deployment of front-haul mid-haul and back-haul with the goal of meeting the critical latency requirements of Ultra-Reliable Low Latency (URLLC) services and efficiency in handling the voluminous traffic generated by the Internet of Things such as Massive Machine Type Communications (MMTC) and enhanced Mobile BroadBand (eMBB).

[12] Think of the sensors on the Internet of Things that generate data and benefit from the results of computing functions.

The management of the data flow between the device, the network, the edge, and the core, where parts of the application and data reside, becomes critical and thus of paramount importance becomes the evaluation of the security issue.

Edge computing can become a critical enabler of blockchain technologies both at the protocol level (between the user and the application) and at the distributed application level across the entire chain between the edges and the core.

In order for blockchain nodes to communicate with each other, data must travel through the entire network and back again, which is how traffic flows in cloud computing. An edge computing network would create mechanisms for new data flows, server to server, eliminating the need for data to travel through the core network.

One of the challenges of edge computing in the world of telco operators is to create a business model that facilitates developer access to edge cloud infrastructure. There is a risk that the edge computing infrastructure will remain fragmented among telco operators, meaning that an application developer would have to interface with each telco operator to ensure that the application works. Otherwise, the developer risks not being able to ensure a consistent (low latency) experience.

The blockchain could be used to securely distribute applications between the various edge nodes of different operators ensuring their "data sharing" and together with multi-cloud could create a decentralized market for edge computing that combines edge infrastructure providers with those who require it.

Especially in peripheral areas, far from the centers of big cities and metropolis, edge computing is one of the most evident examples of how technology can be exploited to bring a real improvement, through different ready-to-use solutions.

One of the most interesting application areas for edge computing is the healthcare sector, where decentralized computing could help accelerate machine-to-machine and machine-to-person communication, providing medical applications and services and distributing workloads in small local data centers. IoT healthcare devices, when interfaced with peripheral data centers, can extend medical staff action to patients in areas with poor connectivity.

Also in the smart city arena, decentralized computing systems can be used in smart urban centers to generate real-time information about traffic trends through devices such as cameras and traffic lights.

The same technologies can be used to create intelligent services to manage the traffic itself.

In fact, there is and will increasingly be a significant volume of data being produced by IoT sensors at all types of endpoints, from traffic lights to trash cans. For this information, peripheral processing enables cost containment as well as service efficiency.

Finally, another field of application for edge computing technologies is gaming, where at the moment the most common solutions are centralized ones in which users connect directly to the core data centers that process the game, with obvious latency problems. By connecting locally to the edge network instead, users would experience very low levels of latency. This is why gaming companies are beginning to experiment with edge computing usage models whereby the customer uses their graphics cards in the cloud, making data processing on the customer's device more streamlined (and effectively expanding gaming usage to those who can't afford computers with expensive graphics cards).

1.5. Data Security and Resilience in the Cloud System

The issue of data security and resilience in the cloud is a topic of absolute importance, which must be carefully evaluated in any business choice regarding cloud services, and which must be addressed according to the usual categories (at least in the context of IT security) of physical security and virtual security at the various infrastructure levels.

As far as physical security and infrastructure robustness are concerned, it is necessary to make sure that the Data Centers and Cloud platforms where data are hosted guarantee the highest degree of reliability both in terms of service levels and in terms of physical and virtual access security. In terms of the first point, it is necessary to guarantee the redundancy of network connections and that of the energy supply infrastructure. Both must be able to cope with multiple failures, guaranteeing in any case the safeguarding of data and, in the most critical cases, the safe shutdown of servers avoiding data corruption. It is also necessary to verify that the Data Center has adequate fire prevention systems and temperature and humidity control. In the event that Disaster Recovery and Business Continuity services are guaranteed, it is essential that the physical distance between the infrastructures guarantees the correct functionality of the services. For example, in order to guarantee Disaster Recovery there should be at least 100 kilometers of distance between the Data Centers that provide the service, while for

Business Continuity it is necessary to guarantee latency times of a few milliseconds, a parameter that varies according to the applications that need to be managed.

For security purposes it is then of extreme importance the availability of a backup system that makes use of:

1) backup technologies different from those used for production disks, in order to avoid that in case of software or hardware malfunctions, the damage is also propagated to the backup systems;

2) encryption of the data both during its transfer and during storage on another device;

3) A backup system that provides varying degrees of data copying and retention. (Rule of 3-2-1);

4) A method of saving backup data on disks and in premises other than those in which the production data resides, and which guarantees that at least one of the copies resides in a Data Center other than the production Data Center;

5) A monitoring system that ensures that the backup is performed correctly and that the backup data is not corrupted.

The latest events in the Cloud world make us understand how often these prevention measures that seem trivial, are often underestimated or applied only in part by those who provide Cloud services.

Still on the subject of physical and virtual security of access, it is important to ensure that Data Centers have a garrison or a remote monitoring H24 that allows access control to infrastructure and private areas (cage) dedicated to data. Access to these infrastructures must be regulated and guaranteed only to personnel authorized to perform certain tasks.

Within Cloud infrastructures, there are several security systems that can guarantee the protection of virtual environments. By way of example, there are solutions that deal with platform access through special Key Access Management, Identity Access Management and Access Control systems.

The most widely used solutions to ensure perimeter security, such as Firewall and Antivirus and Anti-Spam protection are now standard in Cloud infrastructures. However, the offer and implementation of these systems must be carefully verified with appropriate control, correlation and log management mechanisms that guarantee effectiveness in preventing attacks.

Finally, given their frequency, the so-called Distributed Denial of Service (DDoS) cannot be underestimated. These are the most frequent attacks used to damage companies and their business and are carried out by saturating server connections with abnormal amounts of internet traffic, in order to congest the platform and not allow users to access them correctly. To this end, Cloud platforms must adopt DDoS mitigation systems such as scrubbing centers and detection and cleaning tools.

In order to untie some security management functions related to access from the responsibility of the cloud service provider, specialized players have emerged: Cloud Security Access Brokers (CSABs), as defined by NIST. CSABs use tools that can be deployed in the cloud or on private sites and offer services that interpose themselves between customers and service providers with the goal of providing third-party support independent of the cloud provider to implement the customer's security policies, using mechanisms and controls based on risk analysis applied to the data that is stored and processed in the cloud. The services offered by CSABs were created precisely to fill some of the gaps in visibility, compliance, data security and threat protection for cloud-based services. The third-party status of the CSAB vendor with respect to cloud providers offers guarantees against possible risks of abuse by employees who are responsible for the operational conduct of systems at cloud providers (by implementing a separation of duties specific to the management of security measures, such as access management, credentials and encryption keys).

Chapter 2.
“The "legal-economic" regulation of the cloud: the issue of data

2.1. The "traditional" approach to market regulation

Should one wish to address the issue of data regulation, with specific regard to the issue of access, a first hypothesis to be considered concerns the inclusion of the cloud market and/or the data market in the list of electronic communication markets subject to ex ante regulation by the European Commission. Obviously, as a preliminary step, it would be necessary to demonstrate the traceability of these two markets to a broader perimeter of electronic communications: a challenging issue, which is not intended to be addressed here, also because of the conclusions reached regarding the feasibility of this path.

The list of relevant markets susceptible to ex ante regulation has been updated several times by the European Commission, by means of specific Recommendations: the number of markets initially identified in 2003 has thus fallen from eighteen to just four, i.e. those that are currently regulated, whilst the next step is to reduce it to just one market to be subject to ex ante regulation (the fixed access telecommunications network). The Commission's approach has been one of gradual elimination, with some refinement in the definition of the markets themselves, testifying to the effectiveness of the approach followed for the regulation of electronic communications markets. In extreme synthesis, more than three quarters of the markets initially identified have gradually become competitive, and therefore entrusted to the supervision of the competition authorities, as there are no longer grounds for ex ante regulation.

Having said this, it appears highly unlikely that the Commission will proceed in this direction, i.e., to integrate the list currently in force. This is for two reasons. In the first place, as mentioned, the strategy followed by the Commission from the outset is to reduce, to the point of possibly zeroing out, the list of markets subject to ex ante regulation, thus not providing for possible additions. In this sense, it should be recalled that - in the past - on the occasion of revisions of the aforementioned list, indications were received from some stakeholders to extend the list to new services, basically with reference to those offered by digital platforms: in the name of an effective level playing field between operators in electronic communications markets and large Internet platforms (also called Over The Top, OTT), it was proposed - above all - to subject OTT to the same rules as telecommunications companies, but some also suggested considering services such as search engines, distribution of digital content and software, social networks and electronic commerce in the same way as electronic communications markets. The European Commission has never acted on these requests, in the sense that it has never really considered the possibility of extending the list of relevant markets to include Internet products/services.

Secondly, even if it were to revise the approach followed so far, to include the cloud and the - more complex - data markets in the list, the Commission would have to first conduct the three criteria test[13],necessary to conclude that only ex ante regulation could resolve the competition and consumer protection issues (if any) identified.

Now, as far as the cloud market is concerned, defined in the first instance as a single aggregate, without therefore proceeding to the necessary articulation in distinct

segments/markets, a significant role of some non-European operators in the various realities of the member countries is certainly observed; however, rather than a dominant position of a subject, it seems more plausible to define an oligopoly restricted to a limited number of companies. In relation to the discipline of oligopolies, however, the European Commission has not, up to now, developed a position as solid as that of market dominance - single or joint.

These considerations are even more pertinent in the case of the data market, for which an articulation by product seems even more opportune: in fact, there are numerous companies which, in addition to digital platforms, are in possession of extraordinary quantities of data - personal and otherwise - on which they build business models and innovative services. A sector-by-sector approach is the only plausible one. In fact, in some sectors, such as the payments sector, a specific discipline has been in place for some years now, which makes it compulsory to give access to the information held by banks, with the aim of promoting innovation and competition in the payment services markets and - more generally - in the credit market[14].

In conclusion, in the light of the strategy followed so far by the European Commission to reduce the perimeter of the electronic communication markets subject to ex ante regulation, as well as considering the market structures that - prima facie - seem to exclude the existence of single or joint dominant positions in the cloud and data

[13] A clear exposition of the methodology to implement the three-criteria test is represented in BEREC's Guidelines related to this topic. Preliminarily, BEREC recalls that "Consistent with the 2003 Recommendation, the new document refers to the application of the following three criteria to determine whether a market is a suitable candidate market for ex ante regulation: (a) the presence of high and non-transitory barriers to entry; (b) a market structure that does not tend toward effective competition over the relevant time horizon; and (c) the lack of competition law alone to adequately address the market failure(s) in question.".

[14] This is the Directive called PSD2: Directive (EU) 2015/2366 of the European Parliamentand of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

markets, at least if considered as macro-aggregates, it seems highly unlikely that - even in perspective - the cloud and data markets - or their articulations - will be included in the list of electronic communication markets susceptible to ex ante regulation.

In fact, the European Commission - for reasons of competition and consumer protection, but also of competitiveness - is defining a different and more articulated strategy to intervene in the cloud and data markets. The levers used are two: one of a regulatory nature, but with a different approach from the regulation of electronic communications markets; the other of an industrial profile, aimed at strengthening European industry.

With regard to the latter, we will develop some considerations in chapter 3, while in the following we give an account of recent EU regulatory initiatives.

2.2. The regulation of digital services and markets

More precisely, under the first profile, the Commission has just published three proposals for the regulation of digital services and markets, with significant impact on the data market, and - as a consequence - on that of cloud services.

The proposed regulation on digital services, the so-called Digital Services Act Digital Services Act[15], affects all operators regardless of their size and is essentially aimed at:

i. ensure greater online security, so as to increase user confidence;
ii. clarify responsibilities related to the provision of digital services by digital intermediaries (especially online platforms);
iii. reduce the regulatory fragmentation present in member states' markets;
iv. ensure greater transparency in the functioning of digital platforms, in particular with regard to the way they use their algorithms;
v. achieve "equal regulatory treatment" between offline services and equivalent online services;
vi. tackle illegal or otherwise harmful uses of digital services.

The proposed regulation on digital markets, so-called Digital Markets Act[16],

[15] European Commission, Proposal for a Regulation of the European Parliament end of the Councilon a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Brussels, 15.12.2020, COM (2020) 825 final.

[16] European Commission, Proposal for a Regulation of the European Parliament and of the Councilon contestable and fair markets in the digital sector (Digital Markets Act), Brussels, 15.1.2020, COM(2020)842

complementary to the DSA, is primarily aimed at strengthening European antitrust when confronting the market power acquired by large digital platforms (called gatekeepers[17]).

The strengthening of antitrust instruments is, however, accompanied by the provision of ex ante regulation, limited solely to those parties designated as gatekeepers. The main obligations for these companies concern:

i) the use of data, due to the enormous amount of data collected and held, with strict constraints on their use when this may lead to competitive distortions in downstream markets;

ii) (ii) interoperability, with an obligation to provide it to competitors whenever a gatekeeper offers a service in a different market (e.g., in the case of a payment service);

iii) the self-preferencing function, i.e. the obligation for the gatekeeper to modify its own search algorithm in order to eliminate the (widespread) practice of giving preference to its own services over those of competitors.

The third legislative proposal, called Data Governance Act[18], defines an appropriate regulatory framework for data governance, access and reuse (business-to-business, business-to-government, within government).

Among others, of particular interest are:

i) the creation of the figure of the data intermediary, with the obligation for each Member State to notify Brussels of the entities qualified as such;

ii) general legislation for data sharing, in addition to those already envisaged or being defined at sectoral level;

iii) the establishment of appropriate supervisory authorities at both Community and national level.

As far as the first relevant proposal is concerned, that is, the institution of an intermediary of the data, it will be opportune that, in the course of the debate with the stakeholders and in the confrontation with the European Parliament and Council, the Commission considers the - different - relevance that this figure can assume with reference to the typology of enterprise user of the cloud services.

In extremely simplified terms, the "large clients" of sectors such as energy, transport, telecommunications - to remain in the ambit of the network industries - have by now

final

[17] In order to identify these players, the Commission proposes a set of criteria that address their size, role, and the "persistence" of their market power over time.

[18] European Commission, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), Brussels, 25.11.2020, COM(2020)767 final.

matured significant experience in relations with the hyperscalers, while, certainly, for the fabric of small and medium-sized enterprises that characterizes the Italian economy, this intermediary could assume an important significance, reducing the information asymmetry from which they suffer and increasing the bargaining capacity. In any case, as will also be discussed in chapter 4, even for larger enterprises with an already well-established transition to the cloud, forms of cooperation could be useful, with the exchange of best practices, and the strengthening of their own bargaining power so as to balance that of the hyperscalers (countervailing buyer power).

With this legislative package, the European Commission followed up on the initiative launched in February 2020, in which the European digital strategy was updated (redefined, actually) with the programme 'Shaping Europe's Digital Future'.

The new strategy was described as a step-by-step process, of which the first two steps were immediately promoted: i) the Communication 'A European strategy for data', subject to public consultation; ii) the White Paper on Artificial Intelligence ('A European approach to excellence and trust').

Furthermore, the Commission undertook to present, by December, a Digital Service Act, which - in the course of the year - took on a different physiognomy, more ample, compared to that initially outlined, to arrive at the three proposals of regulations just described.

The different articulation of the Commission's programme is also due to the need to take into account the parallel initiatives of other Western countries, aimed at tackling the power assumed by the large online platforms. In particular, the number of investigations against Big Tech in the United States has multiplied, while the United Kingdom came up with a proposal for a regulation a few days earlier than the European Commission[19].

At this point, it can be argued that the regulation of digital markets, with particular regard to data markets - and the related markets for cloud services - is entrusted to the fate of the three proposals for regulations that will now face the (long) trilogue procedure, to reach, conceivably within two years, their final approval, following a debate that promises to be very lively.

However, given the relevance of the issue and the simultaneous and continuous action of the antitrust authorities, both at supranational and national level, against the large digital platforms, it is plausible that the individual EU Member States, also on the basis of the English example[20], will undertake autonomous courses of reform of the antitrust

[19] Competition & Markets Authority, A new pro-competition regime for digital markets, December 2020.

[20] In the UK, the government has asked the Competition and Markets Authority (CMA) to prepare a report on a new pro-competitive framework for digital markets. The CMA, in coordination with the privacy and regulatory authorities (Ofcom), presented a proposal, which was discussed at Astrid, during a seminar introduced by the CEO of the CMA.

discipline, with the attribution of regulatory powers to the respective competition authorities. This is the path chosen, for example, by Germany, where the amendment of antitrust law is currently being discussed, assigning regulatory powers to the *Bundeskartellamt*.

At this point, should other Member States decide to anticipate the European path with national initiatives, there would be a risk of being faced with a further fragmentation of the regulatory framework for digital markets, i.e. contradicting the basic aim of the European Commission's new legislative package: the promotion of a unitary level playing field, in order to offer users and businesses a clear and effective regulatory framework.

Chapter 3.
The competitive structure of the European cloud market: possible evolutions

3.1. A general framework

The issue of data and cloud services is not only the subject of regulatory intervention. In a less organic manner with respect to the regulatory approach, the European Commission is promoting initiatives to support the offer of cloud services and the development of a data market able to promote the competitiveness of the European industry and the efficiency of the public administration.

Without claiming to be exhaustive, but only with the intent of an initial recognition of interventions that can be traced within the framework of a European industrial policy strategy in the field of data and cloud services, the following are recalled:

i. the 2016 European Cloud Initiative[21], aimed at strengthening Europe's position in innovation focused on the use and exploitation of (mainly scientific) data and promoting the Digital Single Market;

ii. supporting the development of next-generation technology systems and infrastructure, including by contributing with investments in European High Impact Projects, to build a reliable and energy-efficient European data space and cloud infrastructure;

iii. the EU's willingness to further enhance cross-border data exchange and promote the data economy through the adoption of a framework of rules applicable to the free movement of non-personal data within the EU[22];

iv. launching sectoral initiatives to build specific European data spaces

e.g. in manufacturing, health, mobility, the *" green deal "*;

v. the above-mentioned support for the Gaia-X initiative, by means of the above-mentioned Joint Declaration;

vi. the promotion of the European Alliance on Industrial Data and Cloud, the work

[21] https://ec.europa.eu/digital-single-market/en/european-cloud-initiative.

[22] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free movement of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59); The principle of free movement of personal data is already enshrined in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (GU L 119 del 4.5.2016, pag. 1).

of which is still restricted to a limited number of participants, but which is, as mentioned above, a particularly important project, both because of the size of its budget, as it is linked to an IPCEI (Important Project of Common European Interest), and because of its relations with Gaia-X.

On point iii, it is worth noting the European objective, in the context of the regulation on the free movement of non-personal data, to avoid 'vendor lock-in' practices. Indeed, data portability between companies is increasingly becoming a key determinant in many digital industries, including cloud services. With Article 6 of the Regulation on the free movement of non-personal data, the Commission therefore aims to stimulate the development of self-regulatory codes of conduct at EU level, with a view to creating the best conditions for the development of a competitive data economy and providing industry with a basis for developing self-regulatory codes governing the switching of service providers and the portability of data between different IT system[23].

With regard instead to the last two initiatives, more directly aimed at data and cloud services, it is appropriate to refer to the official texts, with regard to the specific theme of promoting European industry.

In particular, in the note "Towards a next generation cloud for Europe", the European Commission, together with the German Presidency, make the following statements.

- A common approach to building the European cloud supply will reinforce Europe’s digital sovereignty and increase the competitiveness of European business and industry. In parallel, it will support digitalisation for efficient public administrations, better healthcare and a cleaner, more sustainable environment.
- Member States recognise the need for additional investment, enhanced synergies across national initiatives and a coordinated strategy to lead the cloud uptake in the private and public sectors across Europe. In particular, as agreed in the Declaration, the Member States’ joint actions will focus on:

  i. Combining private, national and EU investment in deploying competitive, green and secure cloud infrastructures and services. This will mean pursuing the next steps together with industry and experts to shape the *EuropeanAlliance on Industrial Data and Cloud.*

  ii. Defining a common European approach on federating cloud capacities, by

[23] In the cloud services market, the Commission has launched Digital Single Market Cloud Stakeholder Working Groups, composed of experts and professional cloud users. One of the sub-groups is working on the development of self-regulatory codes on data portability and cloud switching (SWIPO Working Group), while another sub-group is working on the development of security certification of cloud services (CSPCERT Working Group). The SWIPO working group is focusing on the development of codes of conduct covering the full range of cloud services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

working towards one set of joint technical solutions and policy norms in order to foster pan-European interoperable EU cloud services.

iii. Driving the take-up of more secure, interoperable and energy-efficient data centres and cloud services in particular for small and medium enterprises, start-ups and the public sector.

- A European Alliance on Industrial Data and Cloud will be launched by the end of the year. Within this Alliance, interested Member States, industries and relevant experts will work together to design the detailed business, investment and implementation plan to deploy the next generation cloud capacities for the public and private sector.

The initiative - which the working group considers to be of great value, also for its relations with gaia-X - was then effectively launched, with the holding of several confidential meetings that have been held regularly since December, aimed at - at least for now

- the drafting of guidelines on the Alliance's key priorities, with regard to a number of topics: energy, edge and cloud infrastructure, next-generation hardware, data governance and cybersecurity. Representatives from Italian companies in both the telecommunications and cloud sectors are taking part in the initiative.

These brief references to the European Commission's note are - to date - the only occasion in which, beyond the interviews of individual European Commissioners, a community strategy of industrial policy for the cloud is made explicit, alongside the regulatory path.

With respect to this framework, which is still not entirely clear, in chapter 4 we put forward some initial reflections on the evolution of Gaia-X and the European cloud, for discussion with the participants in the research group.

3.2. The determinants of enterprise uptake of cloud services

The initiatives mentioned in the previous section all stem from an awareness of the importance of the role of cloud services in the data economy and the need to equip Europe - recognising that it is lagging behind the US and China - with a globally relevant data storage and management infrastructure. The initiatives mentioned in the previous section all stem from the awareness of the importance of the role of cloud services in the data economy and the need to provide Europe - recognising that it is lagging behind the United States and China - with a data storage and management infrastructure of global importance. After all, while Figure 1, which refers to OECD member countries, shows that at an aggregate level about 33% of companies with at least 10 employees use cloud services, looking at the positions of individual countries, only 22.5% of Italian companies use them, compared to 51.8% in the US and 52.9% in Canada (but also 19.4% in France and 22.4% in Germany).

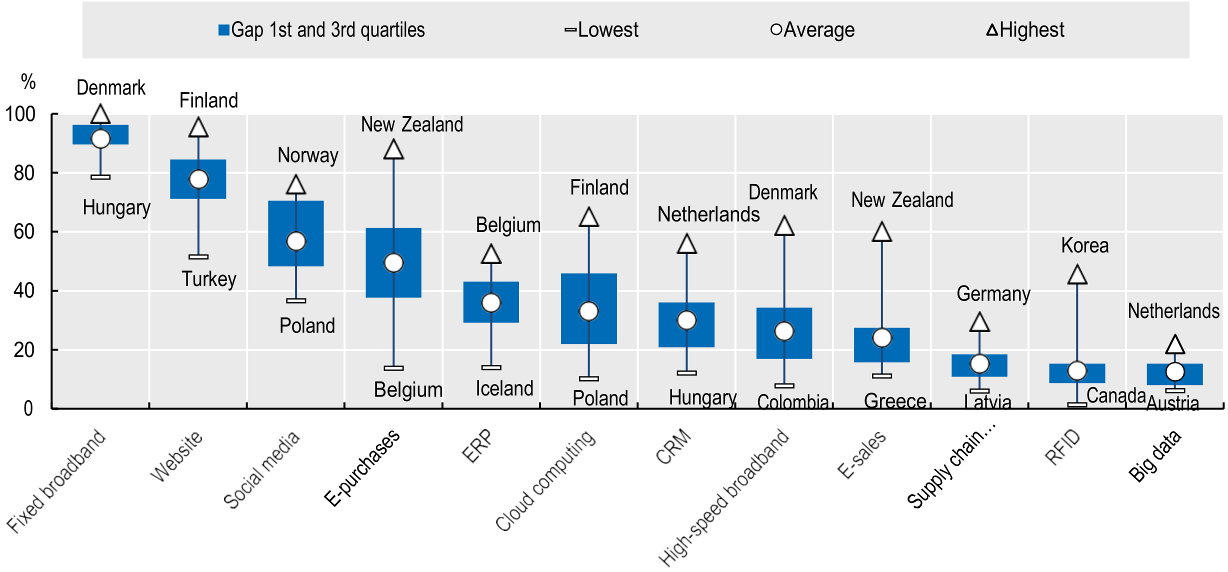


Image 1 – Uptake of some ICT tools and services in enterprises (as a percentage of enterprises with at least 10 employees) 2019. Source: OECD Communications Outlook 2020.

If we want to obtain information on the use of cloud services by Italian companies in greater geographical detail, we can use the first permanent census of companies by Istat, for the year 2018, whose data, as can be seen in Table 1, highlights - also in this field - the delay of the southern regions compared to those of the north. A delay that is more pronounced than that relating to the adoption of management software by businesses, and that could be explained by the greater maturity of the market for management software compared to that of cloud services.

Table 1 - Use of management software and cloud services in Italian enterprises with at least 10 employees, 2018. Source: Istat, permanent census of enterprises.

AREA	**active companies with 10 and more employees**	**active companies with 10 and more employees using management software**		**Active companies with 10 or more employees using cloud services**	
		N.	**%**	**N.**	**%**
Italy	212.396	109.995	51,8%	46.977	22,1%
North-West	68.142	38.352	56,3%	16.664	24,5%
North-east	55.912	30.623	54,8%	13.423	24,0%
Centre	43.555	20.534	47,1%	9.089	20,9%
South	32.322	14.922	46,2%	5.456	16,9%
Islands	12.465	5.563	44,6%	2.346	18,8%

In this context, the efforts of the European Commission to reduce the barriers to the adoption of cloud services by businesses are understandable, which are mainly related to the issues of security and data protection, but also to the uncertainty about where the data will reside, and consequently about the applicable jurisdiction in case of litigation.

In addition, the Commission in 2016 estimated that the total value of cloud services in 2020 in Europe would be EUR 44.8 billion, but more importantly that during the period 2016 - 2020 these services would increase the gross domestic product of the EU28 countries by about EUR 449 billion and contribute to the creation of about 300,000 new businesses (mainly small and medium-sized)[24].

An analysis from an enterprise perspective, to understand the drivers of enterprise adoption of cloud services, suggests that enterprise interest stems from the fact that cloud services allow the transfer of core IT functions into data centres where each physical machine hosts a number of – often very high - of virtual servers. This technological paradigm, thanks to which it is no longer necessary to allocate a physical machine to each server, makes it possible to achieve significant:

- supply-side economies, since as the size of the data centre increases, the cost per server decreases;
- economies on the demand side, since costs depend on the utilisation of IT resources and workloads vary widely over time, requiring large amounts of resources at certain times and virtually no resources at all in the following period, aggregating demand for computing services and diversifying can increase the rate of server utilisation;
- multi-tenancy economies, as application and server management costs decrease as the number of tenants (users) increases.

Supply-side economies derive from various factors, one of the most important of which is the relationship between production scale and electricity costs (which can account for up to 20% of the total cost of ownership of IT systems). In fact, the operators of larger data centres (so-called hyperscalers), as part of their infrastructures, which sometimes extend worldwide, find it easier to locate their installations in areas where electricity costs are lower and, more generally, have a greater capacity to negotiate with electricity suppliers, which translates into lower costs (and prices). The same is true for labour costs: although cloud services allow a reduction in labour costs at every scale of production, thanks to the automation of many system administration tasks, this

[24] Measuring the Economic Impact of Cloud Computing in Europe – A Study prepared for the European Commission, 2016.

reduction becomes even more pronounced as the scale of operations increases.[25].

Costs related to security and reliability of systems, requiring largely fixed investments, also show significant economies of scale. Finally, operators of large data centres can, thanks to their purchasing power, obtain discounts on software and hardware of up to 30%.

Demand-side economies arise primarily from efficiencies in the use of IT resources. In fact, IT costs depend not only on the computing capacity of the systems, but also on the degree of efficiency with which this capacity is used. In a traditional, non-virtualised data centre, each workload, each application, 'runs' on its own physical server, which means that the number of servers varies in proportion to the number of workloads. According to this model, however, servers typically operate at a very low utilisation rate of even less than 10%.

Since in a cloud system several servers are virtualised on a smaller number of machines, in addition to reducing the number of physical machines required, it is also possible to exploit the variability of workloads. There will be workloads that require a lot of system resources at one point in time, but then require none at all; in this context, significant economies can be achieved through aggregation and diversification of demand.

In fact, in a virtualised cloud in which resources are aggregated, first of all - compared to a system based on physical servers - the need to reserve a certain amount of capacity on each server is reduced to cope with sudden peaks in demand (several users performing the same task at the same time).

Since workloads have a time profile (e.g. business activities are concentrated during the day, consumer activities in the evening), reserving one physical machine for each category of application may leave it unused for part of the day, but if the same server (or group of servers) is used for both categories, or the same servers are used for the same type of workload, but in different time zones, the rate of server utilisation can be significantly increased.

Another source of variability that can be exploited to increase server utilisation rates is the seasonality of the business: there are industries such as retail that have peaks at Christmas time, others, such as tax consultancy, are concentrated at specific times of the year. Using the same servers for both activities will increase the infrastructure utilisation rate.

Finally, since computing (CPU), storage and I/O resources are usually bundled on servers in fixed proportions, and since there are workloads that use a lot of computing resources and few storage or I/O resources, and conversely, there are workloads that

[25] Microsoft (James Hamilton, Microsoft Research, 2006) estimates that a system administrator in a traditional enterprise can manage around 140 servers, the same administrator in a cloud data centre can manage thousands.

use a lot of storage and few computing resources, efficiencies can be achieved by running workloads with complementary resource usage profiles simultaneously.

In addition to the supply and demand side economies of scale that can be achieved regardless of the application architecture, multi-tenancy economies can only be achieved if applications are specifically designed to run in a multi-tenant environment, i.e. an environment where it is not necessary to run one instance of a given application (e.g. an Office application) for each customer, but a single instance of an application can be run that is used by multiple users simultaneously (as in the case of shared Office 365).

Multi-tenancy can generate savings in labour costs, since unlike single-tenant environments where application management (i.e. the tasks required to update applications, patch them and troubleshoot problems) has to be done for each individual instance, in multi-tenant environments application management costs are shared among all users using a single instance, driving costs down.

In addition, multi-tenancy also reduces the overhead resources that are usually reserved for running applications. These resources, in a multi-tenant environment, are amortised among all the users of the instance.

Microsoft estimates (Harms and Yamartino, Microsoft Research, 2010) that the combination of supply-side, demand-side and multi-tenancy economies can lead to very substantial TCO savings: Microsoft simulations show that a cloud datacenter of 100,000 servers, compared to a datacenter of 1000 servers can achieve savings in the order of 80%, freeing up resources that can be used for innovation or employed in other activities.

However, reducing operating costs is not the only reason why businesses choose to use cloud services. Other reasons include:

- so-called elasticity, i.e. the ability to scale computing resources up or down quickly - and without changing unit costs (the use of 1,000 servers for one hour costs about the same as the use of 1 server for 1,000 hours), which makes it possible to launch projects that were previously considered too expensive or too time-consuming to undertake;
- the reduction of capital costs, which reduces the costs of starting up or even abandoning projects while encouraging experimentation;
- self-provisioning, i.e. the ability to set up one or more servers via a portal rather than through complex procedures for selecting suppliers and approving expenditure speeds up delivery (and project implementation) times.

What has been said so far about the scale of operations must, however, be balanced with the fact that businesses, as mentioned above, often follow multi-cloud and/or hybrid cloud strategies that envisage, for at least part of their needs, the use of private cloud services; indeed, as can be seen from the latest State of the Cloud report by Flexera[26], relative to the year 2020, these strategies are the norm rather than the exception[27].

While it is true that private cloud services are able to address business concerns about moving their data to public clouds, it is also true that private services, while continuing to benefit from virtualisation and the resulting automation of system management, operate at a smaller scale and with less scope for diversification of workloads. For example, the variability resulting from the seasonality of activities within an individual industry cannot be diversified and therefore the associated efficiencies cannot be achieved.

As a result, the costs of private clouds can be substantially higher than those of public clouds, creating a trade-off between privacy needs, which push towards private clouds, and costs, which push towards public clouds. From this point of view, it is possible that the Gaia-X initiative, by creating a federated infrastructure based on European values, aimed at maximising data sovereignty through interoperability and 'security and privacy by design', could reduce, or at least affect, this trade-off and could even provide new opportunities for those cloud service operators (starting with Telco) located within the European borders whose infrastructures are currently largely unused because users prefer the cloud services of non-EU operators. This is further supported by the aforementioned tendency of cloud infrastructures to move towards the edge of the network, which could favour agreements between Telcos and large cloud service providers.

Finally, it is worth noting that in order for the cloud services market to develop (and therefore for initiatives such as Gaia-X to be successful), companies must be able to easily change cloud service provider, transferring not only their data, but also their IT environments, applications, etc. to the new servers.

For this to happen, they need to be able to converge on a set of well-defined standards

[26] The report was conducted by interviewing 750 managers and users of public, private and hybrid cloud services. The results should be interpreted in the light of the fact that the respondents were from companies with more than 1,000 employees and that only 20% were from European companies (compared to 64% from companies in the Americas).

[27] 93% of respondents to the survey on which Flexera's report is based said they follow multi-cloud strategies, and that 93% of respondents consists of 87% who said they follow hybrid cloud strategies and 6% who said they follow public multi-cloud strategies.

in a short period of time: in fact, although thanks to the use of container-based techniques (such as Docker or Kubernetes) it is possible to transfer one's own applications and workloads from one cloud provider to another, as well as to run applications on highly distributed architectures, in practice this is not always agile.[28] In this respect, an important role could be played by Gaia-X, which, in addition to fostering convergence towards a set of standards, aims to create a framework common to all vertical domains (industry, finance, mobility, green deal, energy, public sector, telecommunications) that should facilitate the creation of an ecosystem of advanced artificial intelligence services, big data analytics, etc. and contribute to innovation.

The creation of this ecosystem could facilitate the transfer of business data from one cloud service provider to another, eliminating lock-in phenomena.

3.3. The cloud for Public Administration: insights for the Italian experience

3.3.1. The history of information technology in PA: an outline

Over the years, the country's public administrations have developed a wide variety of IT systems to support their institutional processes, both at central and local level. In many cases, this has been done by developing custom applications, operating on technological infrastructures managed directly by the individual administration. This has required the creation of their own computer centres to host the technological infrastructures needed to operate these applications. Over time, some services have been outsourced to market players (system integrators), while others have been entrusted to public companies created specifically to manage such systems. In most cases, these systems continued (and continue) to operate in computer centres and on machines of the individual administration.

In order to enable real change and innovation in the functioning of our administrations, it is necessary not only to rethink the nature and functions of these information systems, but also to evolve the technological infrastructures and the related management and procurement strategies, in order to seize the opportunities offered today by the development of the market and to eliminate a series of problems such as the poor security of many IT systems in operation, their high costs and the difficulty of evolving and growing the application pool.[29]

[28] The aforementioned 'State of the Cloud 2020' report by Flexera reports that on average each company uses 2.2 public cloud service providers and 2.2 private cloud service providers.

[29] Astrid began to reflect on these issues back in 2011 with the publication of the book on "*Pubblica Amministrazione che si trasforma: Cloud Computing, federalismo interoperabilità*", edited by Enrico Acquati, Simona Macellari e Alessandro Osnaghi, prefazione di Franco Bassanini e Roberto Masiero, Passigli Editori, 2011.

From this point of view, it is vital for the country's administrations to be able to count on an organic strategy for the adoption of modern cloud computing services and technologies, which would also allow for the reduction and decommissioning of Data Processing Centres (DPCs) and civil structures, which in many cases are decidedly obsolete.

The options available to public administrations are based on two main cases, mentioned above:

1. Private cloud: use of infrastructures owned and managed directly by public administrations or their delegated bodies and companies.
2. Public cloud: use of services offered by market players.

The private cloud ensures that information and information services operate and are managed under the full control of the individual administration. The public cloud makes it possible to optimise costs, increase flexibility in the use of infrastructure services, and take advantage of the experience and technologies of the world leaders in the field.

From the point of view of public administrations, there are cases where it is appropriate or necessary to maintain systems on a private cloud. In other cases, the use of the public cloud can bring a number of significant benefits and should therefore certainly be considered. In reality, the cases in which it is really necessary to use a private cloud are limited, and it therefore makes sense to assume an increasing and broader use of the public cloud.

In general, public administrations should be able to take advantage of both options. In any case, it is vital that all administrations that today have systems and installations in critical situations should and can migrate to solutions that guarantee security, privacy, continuity and organic management of the service.

With regard to the private cloud, some public actors today already have infrastructures capable of offering this service (e.g. SOGEI at central level and several regional or local in-house companies). Some of these infrastructures are of high quality and can certainly constitute a useful resource; others are obsolete and should be decommissioned. In general, it makes sense to think of a rationalisation that qualifies a number of public actors able to offer quality private cloud services.

From the point of view of the public cloud, it makes sense to envisage support for administrations that want to be able to use the services offered by market players.

In recent months, it has emerged that the government intends to create a National Strategic Hub (NSP) to offer cloud computing services. From the documents available so far, a number of points emerge that need further investigation in order to be able to express an opinion on this proposal. Some of these points are highlighted, for which a comparison with the partners in this research would be useful

i. Is the PSN a structure with its own infrastructure or does it act as a broker of existing services?

ii. If the latter, is it only private cloud services or also public cloud services?

iii. Who needs to use PSN services and why?

iv. Does the PSN also offer its services to private individuals?

In overall terms, it is currently unclear what the nature, operating criteria and objectives of the NDP would be and, above all, the relationship it would establish with existing actors.

3.3.2. The rationalization of the IT services of Public Administrations

The use of the cloud, whether public or private, is not simply a matter of technological infrastructure and facilities management (CED). In order to use cloud services, it is first necessary to rethink, restructure and consolidate the application park, so as to make it suitable for migration to cloud platforms and services.

Unfortunately, in recent years, the debate and proposals have focused on the issue of 'reducing and consolidating data centres', without considering that - in the absence of consolidation of the application fleet - the data centre operation is reduced to little more than moving machines, while real migration cannot actually take place.

For these reasons, it is vital that a plan for consolidating and rationalising the application pool of public administrations be drawn up as soon as possible and that a strategy be defined for re-engineering the systems to be migrated in order to make them effectively compatible with cloud platforms, whether private or public.

In the light of the above, it seems appropriate, if not inevitable, that the approach followed for the national cloud project for the Public Administration, envisaged by the Simplification Decree and now, as mentioned, one of the projects of the PNRR, be re-examined.

3.3.3. Italian National Cloud Strategy

The Strategy also outlines the peculiar characteristics of the National Strategic Hub (PSN), a high reliability infrastructure located on the national territory, introduced in Art. 35 of Decree Law 76/2020 (Simplification and Digital Innovation) and included in the PNRR, where in Mission 1 - Component 1.1 (Digitisation of PA) in Investment 1. 1 the lines of the Italian strategy are defined, in particular the 'cloud first' approach to the digital transformation of PA, the rationalisation of data centres distributed throughout the territory and the criteria for the migration of administrations according to performance and scalability requirements and the sensitivity of the data involved.

Introduction

The Strategy points out that most public services are currently provided through PA data centres, which often do not have sufficient characteristics to ensure adequate standards of reliability and resilience. In the Census of PA ICT Assets 2018-2019, AgID points out that 95% of the data centres analysed (1,252) lack the minimum requirements of security, reliability, processing capacity and efficiency. This figure implies that a large part of the digital services offered by the Public Administration to citizens may be vulnerable to cyber attacks, or unable to handle the traffic peaks of its users. The Census also found a low use of the cloud by the public administration.

The "Cloud-First" paradigm, one of the key principles of the Three-Year Plan for IT in Public Administration 2019-2021, is part of this context, whereby in the definition phase of a new project and/or development of services, before any other technological option, PAs are required to adopt the Cloud paradigm.

With the presentation of the "Italian Cloud Strategy", the aspects that will have to guide the safe, controlled and complete adoption of Cloud technologies for the PA are deepened and systematised, with the aim, in the long run, that all the services provided are based on "Cloud-native" applications, i.e. developed natively on the basis of Cloud paradigms.

By 2026, at least 75% of public administrations will have to migrate all their data and services to the cloud, either in the National Strategic Pole (PSN) or in qualified Cloud Services as envisaged by the PNRR.

Between the National Strategic Pole and the migration of the entire Public Administration to the cloud, 1.9 billion euros are available from the PNRR (Mission 1 - Component 1.1 Digitisation of the PA - Investment 1.1 Digital Infrastructure and Investment 1.2: Enabling and facilitating migration to the cloud).

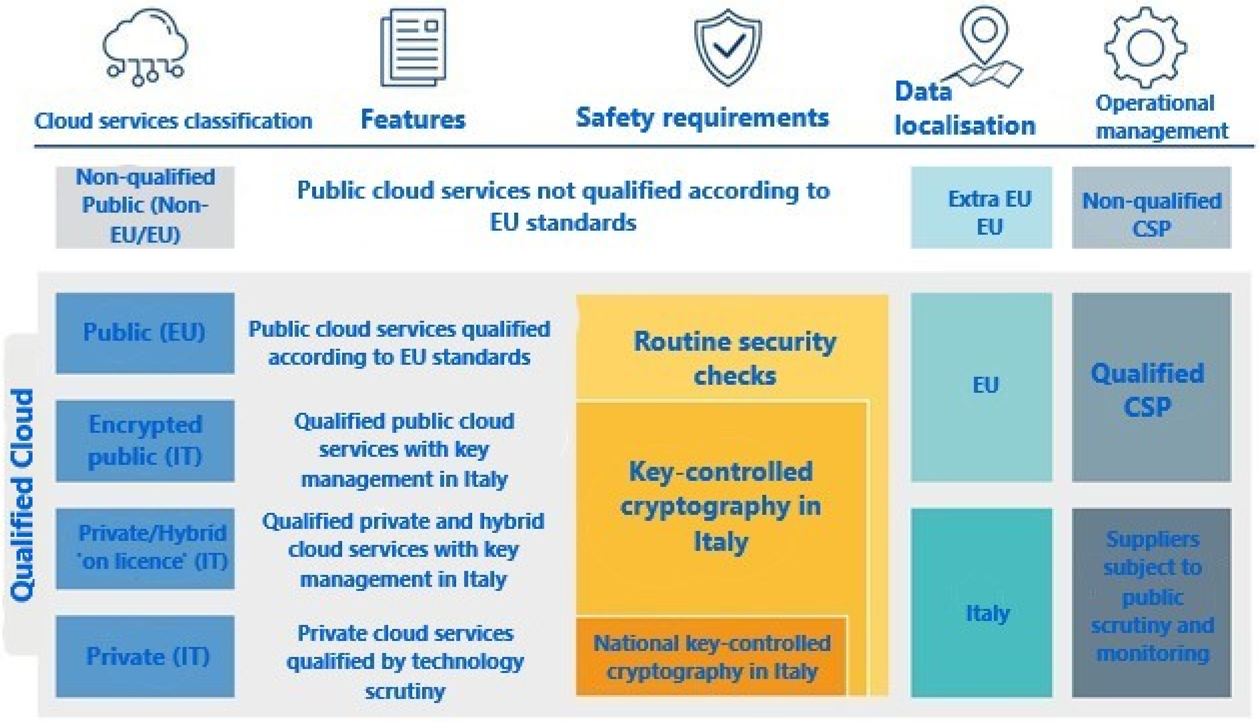
The three pillars of the Italian Cloud Strategy

The Strategy includes three guidelines that will guide the authorities in the choices to be made with regard to the different solutions for migrating to the cloud:

1. **Classify PA data and services** to enable and support migration to the cloud. Data and services will be classified according to the damage that would be caused if they were compromised, i.e. the impact that this would have on the country's system.

2. **Qualifying public Cloud providers and Cloud services** that can be used by PA to ensure that the characteristics and service levels declared are in line with the necessary requirements of security, reliability and compliance with relevant regulations. The qualification of cloud service providers aims to simplify and regulate, from a technical and administrative point of view, the acquisition of cloud services by administrations.

3. **To establish the Strategic National Hub** (PSN), a national infrastructure for the provision of Cloud services, with the highest guarantees of reliability, resilience and independence, whose management and control are autonomous from non-EU entities.



	Cloud services classification	Features	Safety requirements	Data localisation	Operational management
	Non-qualified Public (Non-EU/EU)	Public cloud services not qualified according to EU standards		Extra EU EU	Non-qualified CSP
Qualified Cloud	Public (EU)	Public cloud services qualified according to EU standards	Routine security checks	EU	Qualified CSP
	Encrypted public (IT)	Qualified public cloud services with key management in Italy	Key-controlled cryptography in Italy		
	Private/Hybrid 'on licence' (IT)	Qualified private and hybrid cloud services with key management in Italy		Italy	Suppliers subject to public scrutiny and monitoring
	Private (IT)	Private cloud services qualified by technology scrutiny	National key-controlled cryptography in Italy		

The National Strategic Hub (PSN)

In order to consolidate and secure the PA's digital infrastructures, Article 35 of Law

Decree 76/2020 (Simplification and Digital Innovation) introduced the creation of a highly reliable infrastructure (the National Strategic Pole or PSN) located on the national territory. The development of the National Strategic Pole is promoted by the Presidency of the Council of Ministers, through the Department for Digital Transformation, with the support of the National Cybersecurity Agency.

The aim of the PSN is to host the data and strategic services of all the central administrations (about 200), the Local Health Authorities (ASL) and the main local administrations (Regions, metropolitan cities, municipalities with more than 250,000 inhabitants).

By January 2022, according to Minister Colao, the call for tenders for the implementation of the PSN will be published. The awarding of the tender and the implementation of the PSN is expected by 2022. The completion of the migration is expected by 2025, through a uniform process for all administrations, which will have to start the process of migration to the qualified cloud from the end of 2022.

The infrastructure will be managed by an economic operator selected through the launch of a **public-private partnership** at the initiative of a proposing party. Public and private companies interested in building the National Strategic Hub will then submit an offer of partnership and collaboration, which will then be evaluated by the State. The project is **not open to non-EU players**. At this stage there are three groups vying for the cloud of the Public Administration:

- Cdp, Leonardo, Sogei and Tim
- Almaviva and Aruba
- Fastweb and Engineering.

Data security will be ensured by the approach by design and the adoption of the security requirements of the National Cyber Security Plan and the NIS Directive to enable migration to IaaS and PaaS services. It will also be subject to public oversight, supervision, and monitoring.

The PSN will be geographically distributed over the national territory, articulated in at least four data centres distributed in two regions at appropriately identified sites, in order to ensure adequate levels of business continuity and fault tolerance.

Chapter 4.
First conclusive considerations

4.1. Setting an industrial strategy for the European cloud: beyond the "European cloud champion"

It was planned that by this month, April 2021, the European Alliance on Industrial Data and Cloud would present its proposals for guidelines on the key priorities mentioned above. At this point in time, the working group has not considered these developments, which are moreover unknown. Instead, the working group is exercising - in a completely theoretical way - on the possible paths of a European industrial policy for the cloud, with specific reference to the prospect of promoting an operator in competition with the big companies of the USA and China.

In principle, there is support for strengthening the European cloud and data industry and data industry, including through the synergy of public and private investment.

However, the hypothesis of creating a 'European cloud champion', capable of competing with the big American and Chinese companies, seems unrealistic. This is for several reasons.

Firstly, the European industry is lagging behind the big international players in the cloud market by 10-15 years. This delay seems objectively unbridgeable, especially considering that this sector is affected by continuous technological progress, but also by evolutions in the same supply models, as depicted above. In other words, in this case, the model of leapfrogging innovation that can allow newcomers to challenge established companies in the market, thanks to the promotion of radical innovations (breakthrough), does not seem possible. It is hard to see which firms could promote radical innovations that would challenge the market power of the large American and Chinese digital platforms, which, on the contrary, continue to be the privileged location for new technological developments.

Secondly, an initiative aimed at the construction of a 'European champion' could - most probably - meet with the perplexity of the European Commission itself, if this project were to lead to a reduction in the degree of competition in individual national markets.

In other words, two different requirements should be balanced, which are in any case related to market structures. On the one hand, the creation of a new player in the cloud market, through a series of mergers & acquisitions, collaboration agreements or the establishment of joint ventures would boost the competitiveness of the market, at least at continental level. On the other hand, this process could reduce the number of alternatives present in the different markets, reducing the bargaining power of customers and also discouraging the creation of new companies.

Moreover, there is a problem of 'political' balance, in the sense that - most likely - the 'European champion' would be a 'French champion' or at most a 'Franco-German champion'. The latest market initiatives of the operator Atos could be read in the direction of reinforcing this particular player, candidating it to take on the role of "European champion" of the cloud. If this were the dynamic, our country, but also others, would have to ask themselves whether Europe's digital independence from the big American and Chinese companies would be effectively resolved in this way.

Finally, it may be useful to recall the French experience in the field of national clouds, as a precedent that is certainly not *successful*.

The idea of creating and managing data centres on French soil to host public administration data dates back to 2009. The idea of creating and managing data centres on French soil to host public administration data dates back to 2009, and the project - called Andromède - was launched two years later. The declared objective was to reserve responsibility for security, reliability and system management to French companies, thus eliminating the risk of access to strategic data of the French public administration (but also of French and European companies) by external parties.

The instrument for implementing the project was imagined as a public-private partnership, with the participation of the major players in the ICT markets, but with the State as the first shareholder.

Disputes between the various private actors prevented the Andromède project from becoming a reality, while the idea of a 'sovereign' cloud eventually took shape in two separate companies, Cloudwatt and Numergy.

The first (Cloudwatt) was created with the participation of Orange and Thales, the second (Numergy) of SFR and Bull. In both cases, the State intervened by acquiring 33% of the capital through the Caisse des Dépôts et Consignations.

However, the State's presence was short-lived: as early as 2015, Cloudwatt became an Orange company and Numergy was acquired by SFR.

From the point of view of the business model, both companies, Cloudwatt and Numergy, adopt a hybrid solution, with an offer aimed at both PA and private companies. In this way, the initial idea of the Andromède project to provide an offer targeted only at the PA was overcome.

In conclusion, the public intervention served - in the end - to support the strengthening of two important TLC operators in the cloud market. An outcome that should be considered with regard to market and competitive impacts, not only with reference to the challenge to hyperscalers, but also to smaller companies that also operate in cloud markets.

A different discourse, which for the moment is only hinted at, may instead involve the demand, rather than the supply of cloud services.

In this sense, one could think of a federation of the main users of cloud services, whether they have developed private clouds or use public clouds. In a nutshell, this federation would stand before the major providers with a strengthened bargaining power and supported by a necessarily European discipline that would define the rules for the provision of cloud services, while respecting European values on security, privacy, data ownership, and environmental protection.

In this regard, it is of fundamental importance to follow and as far as possible, guide the evolution of the Gaia-X project.

4.2. The nature and role of Gaia-X

From the Association's website, we learn that Gaia-X is a project "promoted by Europe for Europe and beyond. Its aim is to develop common requirements for a European data infrastructure. Therefore, openness, transparency, and the possibility to connect to other European countries are central to Gaia-X".

The nature of Gaia-X is becoming better defined as the Association progresses in its operation: firstly, with the appointment of the management team. To date, however, there still appear to be aspects that are not fully defined, which therefore still make the various possible paradigms and scenarios from which the working group started plausible:

1. GSM-like" option: in this scenario, Gaia-X is a set of quality, security and interoperability standards that qualify existing offerings, while making them substitutable and interchangeable.
2. Airbus-like" option: In this scenario, Gaia-X is a market player offering with its own facilities cloud services in competition with existing market players.
3. Hybrid" option: in this scenario Gaia-X defines a standardisation and brokerage role towards market services.

In option 1, Gaia-X does not play an active role during the service process, leaving the overall management to the provider adhering to its standards. In Option 2, Gaia-X is a market player offering services to public and private customers with its own infrastructure and capabilities.

Option 3 could be activated selectively for certain market segments. For example, in the case of public administrations, an ad-hoc vehicle could be set up (with a time horizon of no more than 5-10 years) to acquire services from the market through a public procedure and provide them with mixed public-private governance and management, in order to provide greater protection to public customers for critical applications for which the contractual clauses and traditional management models offered by public cloud service providers are not sufficient.

However, this option could in turn be made explicit in (at least) two different ways: in the first case, the public procedure selects "once and for all" and upstream one or more providers that constitute the private core of the public-private partnership; in the second case, the procedure defines a set of constraints, processes and requirements, and all providers that at any given time comply with these requirements could be included as partners and service providers. In the second case, we would be faced with an option that in fact constitutes a reinforcement and institutionalisation of option 1 (there is a managing entity), with particularly stringent requirements and constraints for a specific market sector. stringent requirements and constraints for a specific market sector.

In the working party's view, it seems impracticable to pursue option 2, i.e. the Airbus model, while options 1 and 3 could on the one hand guarantee greater protection for European users and, on the other, pave the way for possible European players who, starting perhaps from niche sectors, are able to become over time a credible alternative to the US incumbents.

It has - however - been mentioned that, following the work of Gaia-X, it is becoming clear that, in addition to the regulatory profile, which in any case differs from that typical of standardisation bodies (e.g. ETSI, for telecommunications), the Association has set itself the objective of creating a software infrastructure logically placed above the physical cloud infrastructures. In this way, we enter the field of industrial intervention, through the promotion of a new European cloud player. This actor would be configured as an enabler of a federation of several 'nodes' (while avoiding hyper-concentration), respecting the criteria of reliability and sovereignty, thanks to the use of software mechanisms, defined by the Gaia-X project, which would guarantee visibility and control over the use of data and a regulation as automatic as possible and based on distributed consensus.

In this context, a project is being developed, this time for the creation of a new physical infrastructure, as part of the Alliance on Cloud and Data Industry, funded through an IPCEI project on cloud[30].

[30] https://www.europeancloudalliance.com/

This issue, together with that of the Gaia-X software platform, deserves specific in-depth studies, which will be carried out in the continuation of the working group's activities.

From the point of view of Italian public administration strategies, it would be useful if the clarifications related to PSN were developed taking into account the evolution of the Gaia-X initiative.

As demonstrated by the first eight business areas identified by Gaia-X to ensure data security and privacy,[31] exposure is not confined to one category: all key sectors from corporate to healthcare, with all their sensitive and private data, are exposed and need protection.

Data is the strategic resource for the digitisation of the economy and will become even more so as Industry 4.0 and IoT grow in importance, bringing to the fore the role of platforms and data exchange as vectors of innovation in strategic areas, from research to artificial intelligence.

Making the best use of this precious resource becomes the primary objective of business ecosystems of all kinds.

And it is in this regard, in defence of the security of companies and States, that the concept of "European data sovereignty" is recalled, which Gaia-X should enhance, together with strategic autonomy and defence of European interests: that competitive role in the Cloud that Europe has not yet been able to play.

In recent years, the European Union has actively intervened in introducing relevant regulatory aspects, raising privacy and regulatory standards, but not in developing the technological credentials (in terms of investment and R&D) to compete with other superpowers, such as China and the United States: an infrastructure gap that Gaia-X seeks to compensate.

The opportunity generated by an effective and sovereign EU infrastructure in which data can be shared and stored according to European protection standards opens up several scenarios; it can give industry and citizens greater confidence in the way data is processed. In the long term, the shared Cloud could foster the development of even the smallest companies, in sectors ranging from finance to energy, giving them the opportunity to present themselves on the global stage and exploit the innovative potential of data, as well as PAs.

With respect to the development prospects of the Cloud industry, the emphasis is, from many quarters, on the importance of the exploitation (and subsequent monetisation) of the data that are stored in the Cloud. More than the question of the residence of the data

[31] Energy, finance, health, Industry 4.0/SMEs, agriculture, mobility, public sector, home automation

on the national territory, the real challenge appears to be - precisely - that of guaranteeing the ownershiṗ and the exploitation of the data produced by businesses and public administrations, defining a discipline that accompanies and integrates the provisions of the General Data Protection Regulation (GDPR), which are limited to personal data.

In this respect, it is of paramount importance to address the issue of data classification, as happened for instance in the experience of some European countries (United Kingdom) and the United States. The classification of data is in fact an important starting point for determining what level of control is appropriate to apply to the type of data in terms of confidentiality, integrity and availability according to the risks of the organisation owning the data.

Still from the point of view of the role of the Italian Public Administration in particular, in the context of the cloud strategy that the new Minister for Innovation and Digital Transition will have to define, it becomes fundamental to also take into account the synergy between the enabling structure and the role of the Public Administration in the digitisation processes, as will be indicated in the PNRR (National Recovery and Resilience Plan).

In this regard, it should be recalled that government action, both at central and local level, has often been centred, even recently, on the new technologies to be adopted and on the development and provision of front-end services (portals, apps, payment systems, digital identity) and not on the re-engineering and review of PA processes and products[32].

A change of perspective of this kind would create the conditions to finally enable direct communication between administrations and, from the IT point of view, the full interoperability of back-ends, the consolidation of the country's databases, and the rationalisation of applications, the latter being an indispensable prerequisite also for the transition to the cloud and the optimisation of the administrations' data centres and processing systems.

In this perspective, as mentioned above, the public sector should increasingly focus on the management of the country's strategic assets (databases and back-end systems), leaving room for the private sector to provide front-end services. In the - very particular - circumstances in which, instead, the State decides to operate in the market with its own offer, it will necessarily have to deal with market conditions, in compliance with the regulations in force and the antitrust rules.

[32] These subjects (in particular the distinction between front-end and back-end and the need to make PA back-ends interoperate in order to develop truly useful front-ends) were already present in the Action Plan for e-government drawn up in 1999 by Prof. Alessandro Osnaghi on behalf of the Minister for Public Administration Franco Bassanini and presented in 2000.

The technical aspects of Gaia-X provide an opportunity to develop at the same time, and primarily, the dimensions of value generated for enterprises and public administrations.[33]

In particular, the architectural standardisation of the so-called federation services enables the creation and management of digital ecosystems by exploiting the interoperability and technological portability that enables dialogue between different actors.

The decentralisation of the Gaia X initiative with the presence of federation services provides the central building block that brings the market model to be innovative for business-to-business digital products.

- It is a marketplace in that it defines rules and software architectures for distributing and exchanging B2B digital products in a competitive and open environment (at least in its broadest and most complete version, as discussed below).
- It is a model in that it can be instantiated in different contexts and environments, without close ties to a single operator.
- It is innovative because it aims at distributing digital products through modern sales, provisioning, cand management mechanisms.

Taking the mobile app stores as a model, it can be said that Gaia-X similarly enables the exchange of digital assets with a focus on business-to-business markets. The technological architecture used therefore does not aim at the front-end, and the end consumer, but at the back end favouring technological interoperability between different systems and allowing migration of infrastructural service providers.

It is therefore possible to state that the Gaia-X model allows a range of three types of distributable products. The first are the downloadable information assets, i.e. digital assets, such as public data sets, ontologies, directly downloadable by users for subsequent processing or analysis.

Then we find the callable application services exposed by service providers and callable by client applications through a machine-to-machine interaction. They allow, in an automated way, to draw on information or functionalities provided by third party systems. They therefore act as connectors applicable to sectors such as banking.

Finally, Installable Infrastructure Assets (in particular, IaaS - Infrastructure as a Service - and PaaS - Platform as a Service) a further layer of digital infrastructure products aimed at offering dedicated capabilities to another party. These include cloud-delivered systems and high-capacity computing systems.

[33] GAIA-X: UN INNOVATIVO MODELLO DI MERCATO PER PRODOTTI DIGITALI B2B – Cefriel, ASTRID RASSEGNA - N. 15/2021

While on the one hand we have the products, on the other hand we have the markets of possible application where Gaia-X acts as enabler.

They can be classified according to their perimeters of use and the consumers within them.

- Enterprise: Marketplaces that enable the distribution of B2B digital products within and between different functions/business lines of the same company, or an ecosystem formed by a group of companies of the same industrial group that exchange assets to create value.
- Inter-company: types of marketplaces that enable the distribution of B2B digital products within specific supply chains. In this case, the partner companies in the ecosystem need to exchange in order to offer an integrated product/service for the creation of which everyone along the supply chain is involved.
- Open: market types that potentially enable the distribution of B2B digital products to all stakeholders.

It can therefore be deduced that an ecosystem of this nature has the potential to create added value by integrating systems that managed in watertight compartments would represent a displacement of value.

From an evaluation of the three market structures in the light of the economic characteristics of the market systems, the authors point out that within the company perimeter there are no conflicts of interest regarding industrial property rights given the closed system. Representing a simplification of the information flow on the one hand, but not a guarantee of effective exchange on the other. There is a general effect of wide benefits generating, positive externalities and spillover effects due to the lowering of transaction costs between the parties and the aggregation and processing of data.

Finally, the open perimeter model sees an open data approach as far as property rights are concerned, as the actors are not always linked by ex-ante relationships. The benefit in this case is the aggregation of different actors resulting in the minimisation of time and costs for accessing data. The peculiar element here is the generation of 'public information goods' that improve the productivity of private actors and the social welfare of public institutions.

In the light of these elements, it is possible to affirm that the interpretation of Gaia-X as an innovative market model for B2B digital products is in total compliance with the European Strategy for Data and its recent regulatory instruments highlighted in the previous chapters such as DGA, DMA and DSA that are being discussed at EU level.