RÉPUBLIQUE FRANÇAISE

Autorité de la concurrence

Only the French version is authentic and it prevails in the event of its differing from the translated version

Summary of Opinion 23-A-08 of 29 June 2023 on competition in the cloud sector

Cloud computing is one of the technological developments that are central to the digitisation of the economy. The cloud describes all the shared services accessible via the Internet, on demand, paid per use and, by extension, some of the underlying infrastructures (data centers in particular). In comparison with traditional IT services, it enables multiple economic benefits for companies. It allows in particular new ways of organising work, based on shared resources that can be accessed remotely.

In view of the functioning of the markets, their importance for the economy and the potential competitive advantages of certain players, it seems imperative that competition on the merits is fully expressed in the cloud sector.

Beyond market failures that can be identified and potentially resolved by current regulatory initiatives, the Autorité has analyzed several risks likely to raise competition issues and presents them in the form of scenarios. These risks may be of a cross-cutting nature, insofar as they globally affect competition in the sector (this is the case, for example, of cloud credits or egress fees). Others are more in line with specific scenarios when migrating to the cloud for the first time or when migrating from one cloud service provider to another. The last scenario examines specific competitive risks linked to barriers to expansion for hyperscalers' competitors. To tackle these risks, the Autorité reiterates that it has several effective and rapid tools to act and protect competition.

Cloud services

The current sector inquiry focuses on public[1] (or hybrid[2]) cloud, which corresponds to commercial offers that give customers direct access to a range of services. A distinction is usually made between three main categories of *cloud* services: IaaS, PaaS and SaaS, that correspond to different shares of responsibility between the *cloud* service provider and the customer company.

-IaaS (Infrastructure as a Service) is the least outsourced model, in which the supplier provides the user with IT infrastructure, such as servers or storage;

-PaaS (Platform as a Service) is an intermediate model. It provides an environment where customers can benefit from software and tools to develop their applications without having to create or maintain the infrastructure or platform usually associated with the process;

-SaaS (Software as a Service) is the most outsourced model. It gives users direct access to applications, managed entirely by the supplier, from any connected device.

The IaaS and PaaS models are distinct from the SaaS model. Customers, uses and business models appear to be very different. Services belonging to the IaaS and PaaS models are mainly intended for IT professionals to build solutions for their own internal and/or external use whereas SaaS services are intended for all categories of users.

IaaS services are the most standardised of all *cloud* services. They represent a small proportion, in terms of numbers, of all public *cloud* services but still accounts for the lion's share of activity and revenues linked to *cloud* services. SaaS services are very diverse.

Use of cloud services

Business customers for cloud services can now be found in all sectors of activity. However, certain highly regulated sectors, such as the government sector, financial services and healthcare, as well as operators of essential services (OES) and operators of vital importance, for example, have to comply with certain constraints that may affect their use of the public *cloud*.

Among all these customers, two categories of operators can be distinguished according to their stage of adoption of the cloud:

- Companies who have chosen to use these services for some or all of their workloads, from an on-premises infrastructure;
- Cloud-native companies are relatively young companies whose entire IT resources have been built directly in the cloud. They have been using cloud services since they were set up and the various workloads have been designed directly using these services. These

[1] Public Cloud: according to NIST, this term refers to products and/or services for which "*the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation,p or some combination of them. It exists on the premises of the cloud provider* ." In contrast, private cloud refers, according to NIST, to products and/or services where "*The cloud infrastructure is provisioned for exclusive use by a single organisationcomprising multiple consumers (e.g. business units) It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises* ."

[2] Hybrid Cloud: according to NIST, this term encompasses products and/or services for which "*the infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability.».*

companies therefore do not have to transform their IT systems in order to migrate to the cloud.

Migration to the cloud concerns large companies as well as SMEs, very small businesses and public bodies, although the criteria for choosing a cloud service provider tend to vary according to the category of customer.

In France, the cloud sector is expected to reach €27 billion by 2025 with an average annual growth of 14%. However, the adoption of cloud services in France is lagging behind, with SMEs and very small businesses migrating more slowly than in the rest of Europe in recent years.

Among French businesses using cloud services (including SaaS) in 2021, the main uses are for document storage (76%) and e-mail (67%).

Finally, companies typically only use one cloud service provider for a given workload. This absence of multi-homing stems from the necessary investments in time, money and technology, the pricing structure adopted by suppliers and the complexity of such projects, for example to ensure the necessary compliance of regulatory standards. Companies can also use several cloud service providers (known as “multi-cloud”) for different workloads.

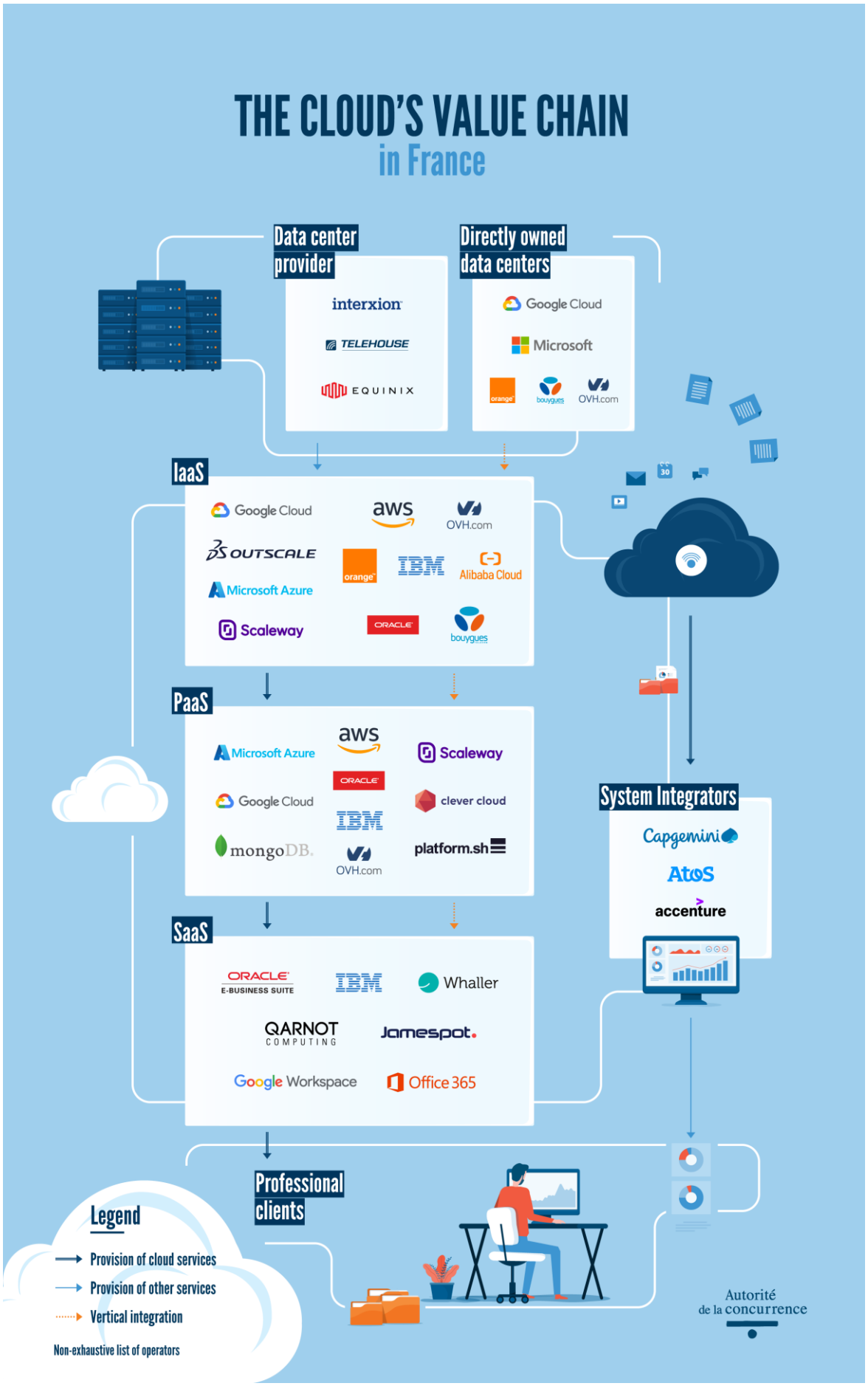
The different operators in the cloud value chain

The operators involved are:

- data centre operators, who build and operate the infrastructures needed to provide cloud services;
- providers already present in the digital sector, such as major digital operators like Amazon, Alphabet (Google) and Microsoft, which have massive storage and computing capacities (known as "hyperscalers"), companies from the software and business information systems sector or electronic communications operators;
- providers active only in the cloud, known as "pure players", insofar as their activities mainly concern the cloud, and where they have little to no presence in other markets. It is the case for example for 3DS Outscale, OVHcloud or Scaleway;
- providers aiming to offer certified "trusted cloud" services (see below);
- IT services companies that act as integrators (and prescribers) or support customers in their dealings with cloud service providers.

Finally, a large number of cloud service providers offer "cloud marketplaces" accessible to third-party vendors. Third-party vendors can generally offer similar services to those of the marketplace operators.

Figure 1 – The cloud value’s chain in France


THE CLOUD'S VALUE CHAIN
in France
Data center provider
interxion
TELEHOUSE
EQUINIX
Directly owned data centers
Google Cloud
Microsoft
orange
bouygues
OVH.com
IaaS
Google Cloud
aws
OVH.com
OUTSCALE
orange
IBM
Alibaba Cloud
Microsoft Azure
Scaleway
ORACLE
bouygues
PaaS
Microsoft Azure
aws
Scaleway
ORACLE
Google Cloud
clever cloud
IBM
mongoDB.
OVH.com
platform.sh
System Integrators
Capgemini
Atos
accenture
SaaS
ORACLE E-BUSINESS SUITE
IBM
Whaller
QARNOT COMPUTING
Jamespot.
Google Workspace
Office 365
Professional clients
Legend
Provision of cloud services
Provision of other services
Vertical integration
Non-exhaustive list of operators
Autorité de la concurrence

The relationship between cloud service providers and their customers

Two main types of contracts are entered into between their suppliers and their customers: on the one hand, in most cases, standard contracts entered into directly on the supplier's website, for an indefinite period and terminable at any time, on the other hand, more personalised contracts for certain key account customers, which are generally fixed-term contracts, varying from one to three years.

Pricing lists for cloud services are published directly on each provider's website. Services are priced on demand and according to usage ('pay-as-you-go' model), whereas traditional IT services charge for the purchase of licences.

Two pricing practices, mentioned in the *Autorité's* Opinion 23-A-05 regarding the French draft law to secure and regulate the digital environment, are specific to the sector:

- Cloud credits allow customers to benefit from reduced expenditure on certain eligible cloud services. Cloud service providers use two main types of cloud credit, which have different durations and values. *Cloud* credits in the form of tests are granted by almost all cloud service providers. These can range from a few dozen euros to a thousand euros and generally last for no more than three months and can be frequent or recurring, with a cloud service provider potentially offering new cloud credits each time it offers a new service. Cloud credits offered in the form of support programs, are offered mainly by larger cloud service providers for users with high innovation potential, such as start-ups, cover much larger amounts (hundreds of thousands of euros, for example) and can last for several years;

- Some cloud service providers, particularly the hyperscalers, are implementing a cloud service delivery model based on billing customers according to their use of outgoing bandwidth, whether it involves data transfers to another provider or to the company's on-premises infrastructures. These pricing structures are called egress fees.

The legislative and regulatory context

This opinion is part of a wider and abundant regulatory environment, with in particular the European Digital Markets Act ("DMA"), which has been adopted in 2022 to put an end to the abuses of the digital giants, and the European Data Act, in the process of being adopted, which aims to promote portability and interoperability in this sector. The French draft law to secure and regulate the digital space also includes provisions relating to the cloud.

How the cloud industry works

The *Autorité* notes that operators such as Amazon, Microsoft and Google, that already have a strong presence in other sectors of the digital economy, have significant competitive advantages over their French and European rivals. These *hyperscalers* enjoy considerable financial muscle, enabling them to make extremely substantial investments that are nonetheless needed to launch activities in the *cloud* industry, such as data centres or IT infrastructures. They can benefit from economies of scale and product ranges linked to the various services offered in their "ecosystems". Finally, they have access to a preexisting customer base that enables them to take advantage of significant network effects, and which can be used as leverage to expand rapidly in the cloud industry.

The French cloud services market, particularly for IaaS and PaaS services, is currently highly concentrated. According to the data sources analyzed by the *Autorité*, the two leading providers, Amazon and Microsoft, will have captured 46 % and 17 % respectively of revenues from IaaS and PaaS services in 2021.

In addition, the major hyperscaler ecosystems are benefiting from most of this growth. The three companies mentioned above are said to have captured 80% of the growth in spending on public cloud infrastructures and applications in France in 2021. The main dynamic in the French market over the next few years could therefore be a trend towards market concentration, to the benefit of the hyperscalers' ecosystems.

The likelihood of a new operator being able to gain market share rapidly appears limited, apart from operators who are already powerful in other digital markets. This probability could be even lower as the number of companies that have completed their migration to the cloud and chosen an ecosystem increases. Indeed, large hyperscalers organised into ecosystems enjoy competitive advantages over suppliers offering more limited catalogues of services, and competitive bidding will generally lead to the selection of a supplier who will cover the customer's entire need, which is akin to competition *for* the market more than competition *on* the market.

These characteristics of the sector are all factors that favour and strengthen the position of existing providers. They call for particular vigilance with regard to changes in the market's competitive structure and to the practices likely to be implemented by hyperscalers.

Analysis of relevant markets in the cloud industry

The *Autorité* finds that customer requirements for cloud services could be formulated in terms of "workloads", which correspond to all the IT resources or business processes meeting a specific customer need or objective. While there are offers with different degrees of added value for the same workload, the analysis of their substitutability will have to be carried out *in concreto*. It would also be necessary to take account of the supply structure when defining relevant markets. In particular, cloud and non-cloud ecosystems could be taken into account in the analysis of relevant markets.

A segmentation based on SecNumCloud certification or "trusted *cloud*" could therefore be considered. Indeed, the "cloud at the centre" doctrine, published by the French government on 17 May 2021, now calls for the cloud to become the default hosting method for all State digital services. In this context, circular 6282-SG of 5 July 2021 specifies that the digital services of administrations will be hosted on one of the State's two internal interministerial clouds, or on cloud solutions proposed by manufacturers satisfying strict security criteria. For example, in 2016, the French National Cybersecurity Agency (ANSSI) drew up the SecNumCloud reference framework to enable the qualification of *cloud* computing service providers. When assessing a possible market segmentation, the *Autorité* could take into account all the circumstances of the case in point, such as the existence of specific functionalities differentiating them from non-certified offers, or a possible price differential,

However, segmentation according to business sector does not, currently, seem relevant.

Lastly, the *Autorité* analysed three types of related markets: the market for data centre colocation services, the markets for on-premise software, in which some companies operating in the cloud markets are also active, and the markets for intermediation in consulting and integration of cloud solutions. It would seem that these markets, and in particular the software market, should be the subject of particular vigilance on the part of the competition authorities, especially with regard to their relationship with the cloud services market. In particular, there could be leverage effects between these markets and the cloud markets, given the dominant position of certain software compagnies who are also present in the *cloud*.

Overall competitive risks

The *Autorité* has analysed a number of cross-cutting practices implemented or likely to be implemented in this sector, which could restrict competition on the merits.

Firstly, the imbalance in relations between customers and hyperscalers can be seen in the presence of certain key operators in the market, which can even make it difficult for powerful customers to negotiate contract clauses. Secondly, it can be difficult for customers to anticipate future cloud costs, given the complexity of the offerings and the lack of pricing clarity.

Cloud credits and egress fees also caught the *Autorité's* attention.

Cloud credits are of real use and added value for many companies, especially startups, who can avoid substantial investments that could hamper their development, but also for cloud providers, who use them to spread and encourage adoption of their technology.

However, the *Autorité* considers that special attention should be paid to targeted support offers. The sometimes high amounts offered, the vast ecosystem of companies they cover and their validity periods set them apart significantly from the free trials that can traditionally be seen in other industries, and raise doubts about the ability of all cloud providers to offer them profitably.

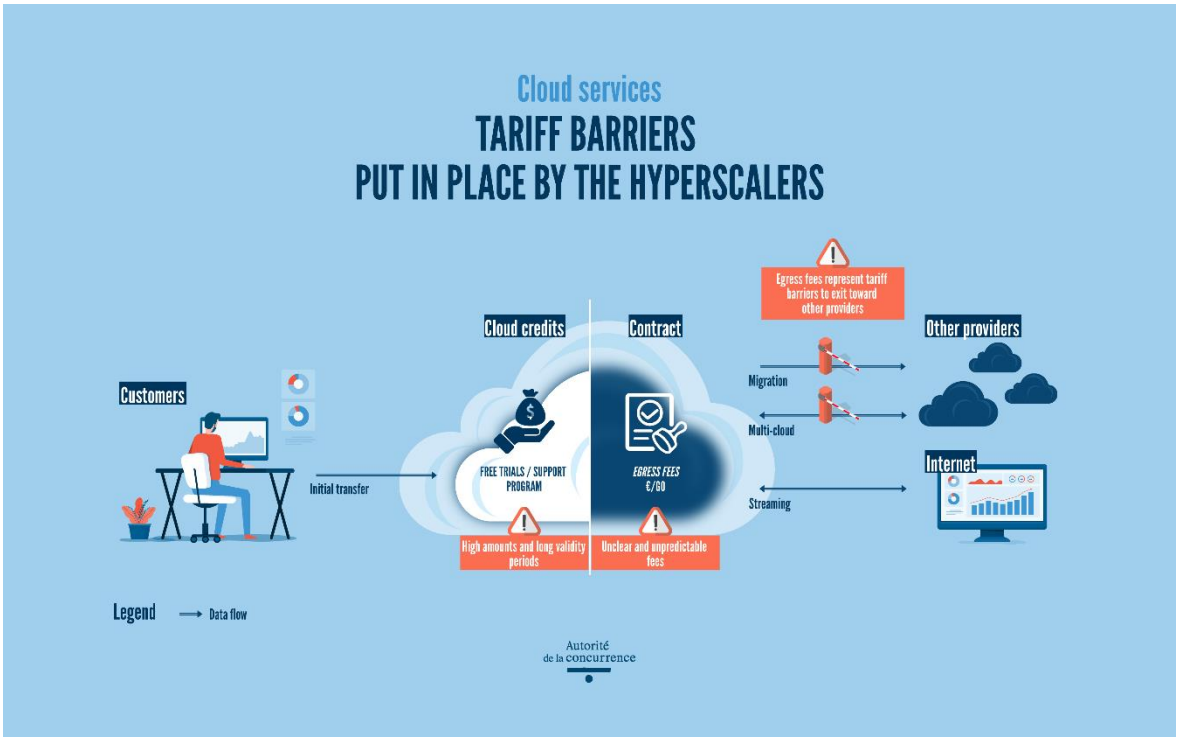
Furthermore, given the time-consuming and costly developments required by customers to set up a cloud architecture with a specific provider, and the technical and financial costs associated with migration, there is a risk of lock-in by the major providers. This practice, which is causing concern among market operators, could have even greater negative effects as it primarily targets customers with a high potential for development and innovation. This lock-in could be reinforced by the presence of clauses or practices limiting the options for changing supplier or using several suppliers simultaneously.

In order to guarantee the benefit of these cloud credits, it is therefore important to ensure that as efficient competing cloud providers are able to offer them profitably.

The investigation has shown that egress fees are potentially disconnected from the costs directly incurred by suppliers regarding data transfers. They are a major concern for the industry, as their pricing structure is proportional to the volume of data transferred, and customers are unable to anticipate their future needs in terms of data traffic and bandwidth usage.

As they are currently structured, these fees could create a risk of customer lock-in on a fast-growing market, by making it more difficult for cloud users to leave their primary provider or to use several providers at once in a multi-cloud environement, for the same workload or for different workloads when they involve recurring data transfers between them.

Figure 2 – Tariff barriers put in place by the hyperscalers



Specific competitive risks

The *Autorité* has identified specific competitive risks in three different scenarios: the situation of customers when they first migrate their on-premise IT to the cloud, when they migrate from one cloud provider to another and the barriers to expansion for hyperscalers' competitors.

Specific competitive risks associated with migrating on-premise information systems to the cloud

Migrating customers from on-premise solutions to the cloud is complex and costly. When making a choice for a cloud service provider, customers may rely on their current IT service providers, especially when they are also cloud providers.

The investigation uncovered practices likely to reinforce the disincentives for a customer to use an alternative cloud provider, such as restrictive contractual clauses, tied sales, pricing advantages favouring their products, and technical restrictions. If implemented by an operator in a dominant position, these practices could constitute abusive practices. Several complaints relating to similar practices are currently being examined by the European Commission .

Specific competitive risks associated with migrating from one cloud services provider to another

Impediments to migrating to another provider for already cloud-hosted workloads can undermine the functioning of competition, preventing customers from changing cloud providers.

While many companies are still in the early stages of migrating or developing their cloud solutions, and have not yet considered migrating to another provider, it is already apparent that migration from one cloud provider to another can be hindered by technical barriers, but also by deliberate practices by providers.

Technological barriers to migration can appear at various levels, linked to the specific architecture and solutions used. Indeed, the variety of products and services, especially PaaS services, the interconnection of IT services and the lack of portability of data and applications can lead to significant migration costs. In addition to the technical obstacles, suppliers can put in place certain additional technical and commercial barriers, increasing migration costs in order to strengthen their position. This could be the case, for example, of a dominant company deliberately using a specific data format to prevent the portability of a customer's data to an alternative cloud provider. Providers may also be able to impose commercial conditions that contribute to locking customers into their ecosystem.

Specific competitive risks linked to barriers to expansion for hyperscalers' competitors

The sector is also marked by technical barriers to interoperability. These affect all competitors, but they have a greater effect on smaller providers, given the attractiveness of *cloud* ecosystems when it comes to choosing a first provider. These obstacles are illustrated in the opinion by practical examples, such as the technical implications of interoperability with regard to the Amazon S3 object storage service (IaaS). Interoperability with PaaS services is even more complex, since, for example, changing the PaaS database service requires rewriting the part of the application code that uses that service.

The *Autorité* has also identified several competitive risks.

Firstly, the risks associated with a supplier's presence in several related markets:

- restrictions on competitors' access to the software needed to provide *cloud* services: a software publisher who happens to be a cloud service provider could implement practices aimed at raising the price of the licenses needed by its competitors, or making the use of its software conditional on the purchase of a large number of licenses. In this way, a software publisher in a dominant position on the software market could leverage some of its competitors out of the market, in order to win customers for cloud services.;

- more advantageous commercial or technical conditions for the provider's own products or services: due to their conglomerate structure, hyperscalers can develop discount systems, tariff and non-tariff benefits or cross-subsidies, thus using their market power in related markets to accelerate the development of their cloud service provider activities;

- privileged access to data: hyperscalers benefit from privileged, even exclusive, access to data that is difficult for their competitors to reproduce, and is likely to give them a decisive, competitive edge. This privileged access may stem in particular from the fact that many cloud services use artificial intelligence to exploit data and deliver more sophisticated analysis services to their users. This can lead to better sales targeting and a more detailed understanding of customer needs, as well as improved service functionalities and the development of innovative new tools, such as artificial intelligence or machine learning. These developments can have a positive impact on consumers and innovation. However, they can also lead to a significant competitive imbalance between operators, insofar as the hyperscalers' competitors cannot reproduce this volume of data easily or on the same scale.

Secondly, beyond the impossibility of identically replicating cloud credit offers, particularly for smaller providers, and the impact of egress fees on multi-cloud strategies, the *Autorité* identifies other risks.

While the role of marketplaces in the cloud industry is currently still minor, these are tending to grow in importance, both for the providers of these platforms and for the publishers who offer their services on them. The *Autorité* considers that several competitive risks could emerge, in particular linked to the conditions set by providers for access to and operation of these marketplaces:

- several stakeholders consider that some providers, such as AWS and Oracle, include clauses preventing third-party publishers from communicating or promoting their offers through their services acquired via the marketplace;

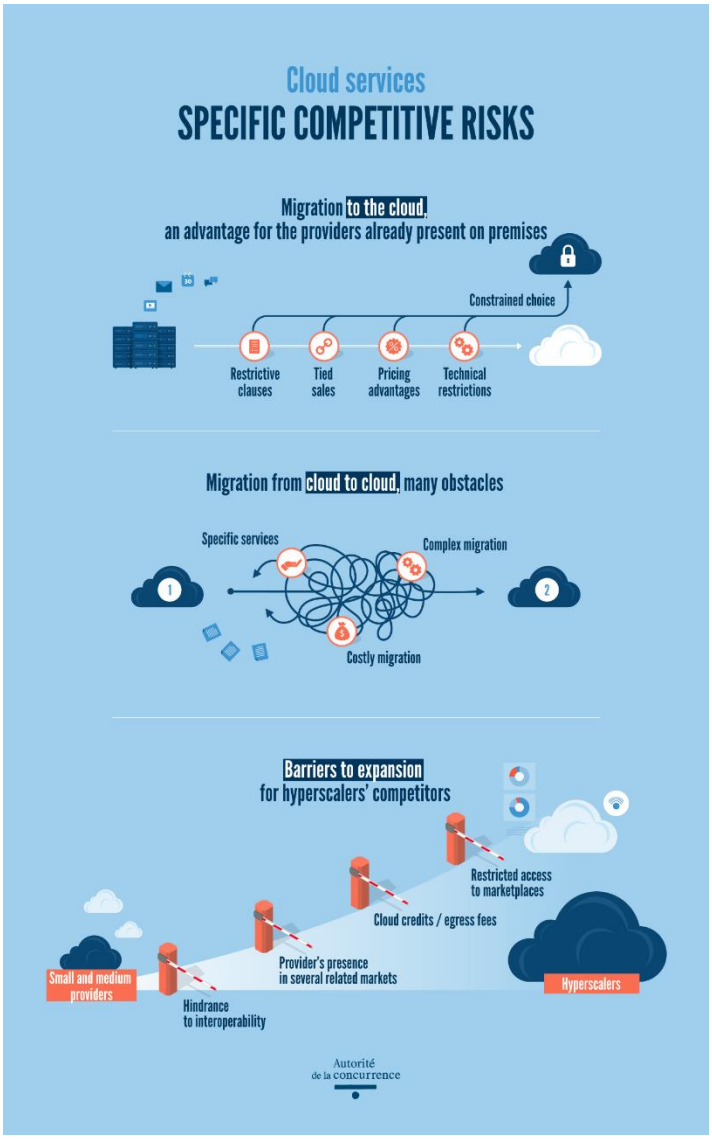
- through the marketplace, the provider can also promote its own solutions, both in terms of marketing and customer promotion, to the detriment of other services offered by third parties;

- tariff parity clauses could also be imposed. Through these clauses, the provider can withdraw the third-party publisher's service from sale when the price on its marketplace is higher than on other marketing channels used;

- it will also be vital to keep a close eye on commission rates, which will be an interesting indicator of the essential nature of certain marketplaces.

Lastly, the possibility of obstacles deliberately being put in place to hinder interoperability cannot be ruled out. Cloud service providers offering particularly popular products or services could prevent or restrict access to key information needed to ensure the interoperability of these products or services with those of their competitors. This practice could have the effect of restricting the compatibility of competing solutions, and hence their attractiveness to customers.

Figure 3 – Specific competitive risks



Competition Law responses

To meet the challenges posed by the cloud, one could consider, alongside the classic competition law tools of abuse of dominant position, combating illegal cartels, merger control and abuse of economic dependences using other instruments from Book IV of the French Commercial Code (Code de commerce),, such as restrictive competition practices,

The competition authorities have a rich decision-making practice that can serve as a reference in the event of an action based on the abuse of a dominant position. Examples include the Google Shopping case in 2021 (in which the General Court of the European Union clarified the issue of discrimination/self-preferencing), the *Autorité's* Nespresso case on tied selling practices (2014) and the Microsoft case (2004), in which the European Commission set out a number of important principles concerning the refusal of dominant companies to provide interoperability information. In addition to the refusal to provide interoperability information, the sharing of degraded or discriminatory information has also been examined by competition authorities. For example, the *Autorité* has raised competition concerns about Meta's practice of degrading intermediaries' ability to provide advertisers with services based on their own advertising technologies (for example, by withdrawing Criteo's access to an application programming interface required for its activities). More recently, in May 2023, the Authority found that Meta had failed to define transparent, objective and non-discriminatory access criteria for its advertising verification partnerships. The *Autortié* therefore enjoined Meta to introduce new criteria for accessing and maintaining these partnerships.

To deal with such situations, the *Autorité* has been able to use effective and rapid procedural tools at its disposal, such as interim measures, used in 2023 against Meta in the advertising verification sector, or commitments, used twice in 2022 in cases involving Meta and Google.

Antitrust law regarding cartels may in some cases be a relevant instrument. Numerous groupings and associations of cloud service providers have been formed in recent years, or are in the process of being formed, with or without the creation of a common legal structure, in particular :

-joint structures between cloud operators to provide "trusted *cloud*" offers;

-technology partnerships between major data-related software vendors and cloud providers. In 2019, for example, Microsoft and Oracle announced a cloud interoperability partnership, enabling customers to migrate to and run business-critical workloads on Microsoft Azure and Oracle Cloud;

-alliances or technological partnerships between integrators and the majority of *cloud* providers, especially hyperscalers.

- specific partnerships in certain sectors.

The fact that, on the one hand, these entities group together autonomous and sometimes competing companies and, on the other hand, that their operation implies contacts between these same companies exposes them to risks with regard to the rules prohibiting cartels.

Standardisation solutions, which at first glance promote interoperability and therefore provider switching could also, in some cases, become problematic on a competition level if it aims to prevent the emergence of alternative solutions and to paralyses innovation through technical lock-in practices,

Competition authorities also need to be particularly vigilant when it comes to mergers.

In recent years, there have been a number of major deals involving cloud providers around the world, such as IBM's acquisition of software provider Red Hat in July 2019, US group Broadcom's planned take-over of VMware, which is currently under scrutiny by several competition

authorities, and Microsoft's takeover of Activision Blizzard, which has raised concerns about the emerging cloud gaming market and led to contrasting responses from the different competition authorities.

During the public consultation, a number of operators expressed concerns about possible concentrations in the cloud industry. Among the main risks identified, they mentioned the reduction in the number of companies, potential bundled or tied sales, a drying up of innovation and alternatives for customers, as well as potential price increases. Several companies also mentioned cases where technology solutions that could previously be integrated with multiple suppliers were transformed into proprietary technologies after a take-over.

More generally, stakeholders expressed the feeling that a concentration dynamic was underway in the cloud industry, particularly on the French market, and that this could continue over the next few years. However, while the largest cloud services providers, particularly the American ones, have all made acquisitions in recent years, it appears to be much rarer on the part of European operators.

Finally, the creation of new entities in the form of joint ventures to offer, for example, "trusted *cloud*" labelled services, is another form of concentration likely to raise competition concerns. Several operators have pointed out the risks to competition associated with the communication and marketing resources deployed to launch their offers and obtain the "trusted *cloud*" label.

Finally, it may be appropriate to consider these issues from a broader angle.

The abuse of a situation of economic dependence may be an interesting approach without affecting current legislation. For the record, this sanctions abusive exploitation by a company or group of companies of the situation of economic dependence in which a customer or supplier finds itself, where this is likely to affect the functioning or structure of competition. This legal basis was used by the *Autorité* to sanction Apple in 2020.

The application by the *Direction générale de la concurrence, de la consommation et de la répession des fraudes* of the law on restrictive practices could also be justified, notably in the context of sanctioning a significant imbalance or a benefit without consideration.

Other responses in the event of market failure

The *Autorité* has also found the existence of market failures that could justify recourse to regulation.

While technical solutions exist to facilitate supplier switching or the use of multi-*cloud* (standard services or open source solutions, for example) self-regulation has not led to the establishment of common technical standards. Incumbent operators, particularly hyperscalers, are not necessarily encouraged to develop high-performance ou best-price solutions if they are likely to erode their market shares. Several customers have confirmed that the major cloud providers are not necessarily looking to offer standard solutions for accessing their cloud services.

In addition, joint initiatives to develop common standards are difficult to implement, such as Gaia-X, initially founded by 22 French and German organisations, and the European SWIPO initiative. Indeed, the presence of hyperscalers in the technical working groups and their supposed desire to slow down or complicate discussions are highly criticised and contribute, according to some stakeholders, to the lack of results from these initiatives.

A regulatory approach therefore seems better suited to address market failures, as European and national regulators have initiated in recent months with the DMA and Data Act, or the French draft law to secure and regulate the digital space recently presented by the government. In its opinion 23-A-05 of 20 April 2023 concerning this draft, the *Autorité* made a number of recommandations

designed to ensure that its provisions are aligned with those of the Data Act and to strengthen the effectiveness of its provisions.

As the trialogue ended on 27 June 2023, it is not appropriate for the *Autorité* to make proposals for improving the current text of the Data Act. However, as the Commission is due to carry out an evaluation exercise in three years' time, the Autorité considers that it is appropriate to monitor several issues (distinguishing the regime applicable to egress fees from other migration costs, carrying out an impact study on cloud credits and specifying measures to promote portability and interoperability).

Perspectives and conclusions

Several developments likely to have an impact on the competitive operation of the industry need to be taken into consideration.

Firstly, as the *Autorité* has shown, competition the cloud industry is characterised by competition *for* the market rather than *on* the market insofar as, for a specific need or workload, customers tend to turn to a single supplier, particularly those with an attractive ecosystem. Given the risk of customer lock-in to these ecosystems, customer demand should tend towards a distribution between the main ecosystems, with only slight variations in market share once the bulk of the workload inventory has been dealt with, which could lead to a reduction in competitive intensity.

At the same time, new technologies that improve the performance of products and services are expected to emerge, and potentially change the structure and competitive balance of *cloud* markets. Competition authorities will have to remain vigilant to ensure that established players do not hinder the development of smaller or new players based on these technologies.

Firstly, the increasing use of artificial intelligence will drive growth in demand for cloud services. In fact, the countless developments towards increasingly complex models, such as Large Language Models, require considerable computing power.

This is also the case for edge computing, identified as an innovation that will have a major impact in the near future. The ability of cloud providers, particularly non-hyperscalers, to position themselves on these technological challenges could therefore help overcome some of the identified barriers to entry and expansion. Other uses are emerging, such as *cloud* gaming.

Developments in the cloud industry are also likely to be influenced by wider global considerations, such as geopolitical changes, which will potentially impact cloud security innovation or the growing importance of the environmental footprint.

The competitive risks set out in this opinion will be carefully analysed by the Autorité’s investigation teams. This vigilance, which may result in the opening of litigation-type investigations. This review is key to preserving innovation and to minimising costs in an industry that represents a major vector of economic growth for companies.