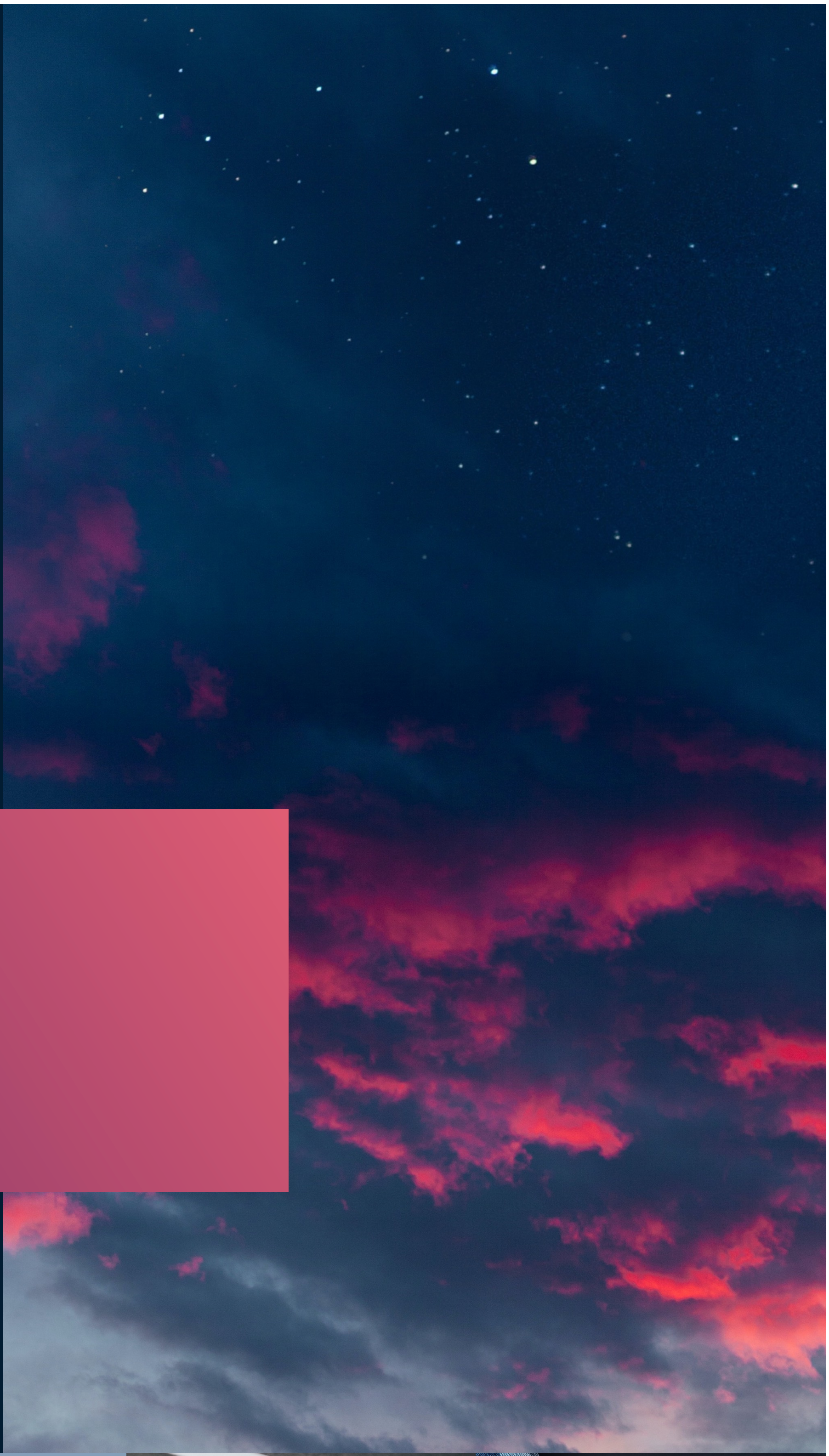
RÉPUBLIQUE FRANÇAISE

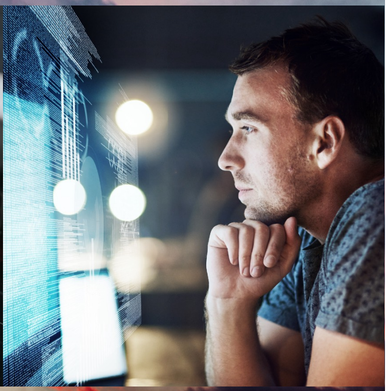
Autorité
de la concurrence

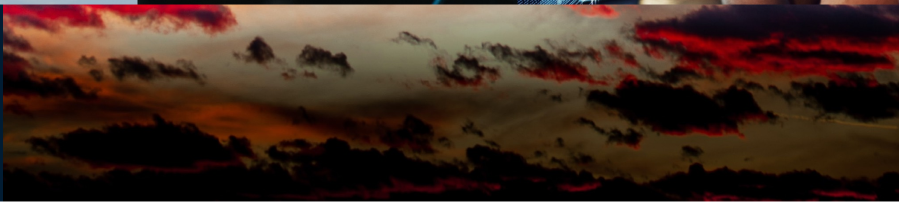
OPINION 23-A-08

of 29 June 2023

on competition in the cloud sector







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

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

The *Autorité de la concurrence* (permanent standing committee),

Having regard to Decision 22-SOA-01 of 27 January 2022 on conducting a sector-specific inquiry on its own initiative in the cloud computing sector, registered under number 22/0007 A;

Having regard to Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act);

Having regard to the proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act);

Having regard to Book IV of the French Commercial Code (*Code de commerce*);

Having regard to Opinion 23-A-05 of 20 April 2023 on the draft law to secure and regulate the digital space;

Having regard to the public consultation paper on the competition in the cloud sector published by the *Autorité de la concurrence* on 13 July 2022;

Having regard to the contributions received as part of the public consultation;

Having regard to the other evidence in the case file;

Representatives of the *Club informatique des grandes entreprises françaises* ("Cigref"), OVHcloud, Scaleway, 3DS Outscale, Google, Microsoft, Amazon and the Directorate General of Enterprises having been heard heard during the hearings on 1 February 2023;

Representatives of the companies Atos, OpenClassrooms and EDF having been heard heard on the basis of the provisions of the second paragraph of Article L. 463-7 of the French Commercial Code (*Code de commerce*);

The case officers, the Head of the Digital Economy Unit and the representative of the minister of the economy having been heard heard during the hearing of the *Autorité de la concurrence* on 28 April 2023;

Has adopted the following opinion:

Summary[1]

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[2] (or hybrid[3]) 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;

[12] 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] 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* ."

[3] 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».*

-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. PaaS 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 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.

♦ *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.

♦ *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.

a. 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 .

b. 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.

c. 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.

♦ *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.

SUMMARY

Introduction

1. Cloud computing, cloud services or simply the "cloud"[4], is one of the technological developments at the heart of the digitisation of the economy. The cloud describes all shared services, accessible via the Internet, on demand, paid per use and, by extension, some of the underlying infrastructures (notably data centres). The cloud offers multiple economic advantages for companies compared with traditional computing. In particular, it enables new ways of organising work, based on shared resources that can be accessed remotely. These characteristics can be sources of productivity gains for companies and value creation for the economy.

2. The cloud industry is part of an ever-changing economic and regulatory environment. In France, this sector is expected to grow by around 14% a year, reaching 27 billion euros by 2025[5]. At the same time, the sector is structured around several categories of stakeholders. In recent years, a handful of "hyperscalers"[6] have concentrated the bulk of the market in terms of both volume and growth. Responses to the issues raised by data protection[7], security and sovereignty will lead to major regulatory changes that are likely to influence market development.

3. Against this backdrop, on 27 January 2022[8], the *Autorité de la concurrence* (hereinafter "the *Autorité*") started proceedings ex officio, based on Article L. 462-4 of the French Commercial Code (*Code de commerce*), on competition in the cloud sector, in order to carry out an overall analysis of how competition operates in this complex, fast-growing technical sector that is expected to create considerable value for the European economy.

4. The purpose of such an opinion is neither to classify market behaviours under Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU) and Articles L. 420-1 and L. 420-2 of the French Commercial Code (*Code de commerce*) nor to rule on notified merger operations. Specifically, it aims to study the functioning of a sector from a competition law perspective, paying particular attention to the impact of recent or current developments[9] on the overall competitive balance of the sector and other economic sectors dependent on it.

5. With this opinion, the *Autorité* has sought to improve understanding of this technical and complex sector, propose analyses to define relevant markets, identify any current or future competition problems and, where appropriate, make proposals likely to improve the competitive operation of the sector.

[4] For a better understanding of this opinion, this term is defined in the glossary available at the end of this document.

[5] Markess by Exaegis - Digital Infrastructures and Cloud - Market Data 2022, 30 March 2022.

[6] A term used for very large companies that have built global hosting capabilities and developed dedicated applications used by millions of users.

[7] See glossary.

[8] Decision 22-SOA-01 of 27 January 2022 regarding the start of ex officio proceedings to analyse competition conditions in the cloud computing sector (link to the press release).

[9] In its Communication on the definition of relevant market for the purposes of EU competition law, submitted for consultation, the Commission gives examples of significant developments to be taken into account: "*these include the digitisation of the economy and new ways of supplying goods and services, as well as the increasingly interconnected and globalised nature of trade*" point 2 (link).

6. In the course of this investigation, numerous stakeholders in the sector were interviewed on the basis of Article L. 450-3 of the French Commercial Code (*Code de commerce*). The *Autorité* exchanged views with both French and international stakeholders from the private sector (providers, customers, associations and others) as well as with institutional stakeholders (sector regulators, foreign competition authorities, ministerial departments). In all, over 40 interviews were conducted during the investigation.

7. With regard to institutional stakeholders, the *Autorité* talked to other foreign authorities that carried out in-depth work on the competition issues raised by the cloud sector:

   - the European Commission (hereinafter the "Commission") has received several complaints concerning potential anticompetitive practices in the sector;
   - the Japan Fair Trade Commission (hereinafter "JFTC") published a report on cloud services on 28 June 2022[10];
   - the Dutch Competition Authority (*Autoriteit Consument & Markt*, hereafter "ACM") published a market study on cloud services on 5 September 2022[11];
   - on 22 March 2023, the U.S. Federal Trade Commission (hereinafter "FTC") launched a call for submissions to assess the functioning of the cloud sector (competition and data security) in the United States[12];
   - the UK's Office of Communications published an interim report on a market study of cloud services on 5 April 2023[13].

8. In addition to interviews, questionnaires were sent out to cloud service providers and customers, as well as to other stakeholders such as system integrators[14] software vendors. An online survey system was used to collect the responses to the questionnaire for cloud service customers. Questionnaires were also sent out to professional associations, in order to receive responses from their members. The investigation services collected responses from over 50 stakeholders.

9. On 13 July 2022, the *Autorité* published an interim document presenting the initial lessons and trends taken from the first six months of the investigation. This document was put out for public consultation[15] until 19 September 2022, to collect comments from all stakeholders. In particular, these stakeholders were asked to give their opinion on the definition of relevant markets and on practices likely to be implemented in the sector. The *Autorité* analysed the 20 responses received and took them into account in drafting the final opinion.

[10] https://www.jftc.go.jp/en/pressreleases/yearly-2022/June/220628.html.

[11] https://www.acm.nl/en/publications/market-study-cloud-services.

[12] https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data.

[13] https://www.ofcom.org.uk/consultations-and-statements/category-2/cloud-services-market-study.

[14] Integrators support cloud service customers in managing their migration to the cloud and in upgrading and maintaining their applications in the cloud in operational conditions.

[15] See the *Autorité's* press release, "*The Autorité opens a public consultation as part of its cloud sector inquiry*", 13 July 2022 (link).

Reminder of the approach adopted by the *Autorité* in the public consultation document published on 13 July 2022

In this opinion, the *Autorité* focuses on the competitive functioning of the public or hybrid cloud and on the IaaS and PaaS[16] models, although developments may concern the entire cloud value chain where these are relevant to the competitive analysis.

With regard to the different players in the cloud value chain, this opinion focuses on cloud service providers in the strict sense of the term. Data centre operators and integrators who do not provide cloud services are therefore not the main focus of this analysis, although incidental developments may be devoted to them.

As far as customers are concerned, this opinion focuses on the relationship between cloud service providers and business customers. The market for cloud services to private customers will not be covered.

Lastly, this opinion analyses the competitive situation primarily in the French market.

10. After an introduction to the cloud sector (I), a section will be devoted to the functioning of the sector (II), followed by an analysis of the relevant markets (III). The *Autorité* will then present the competitive risks it has identified in the sector (IV). Lastly, the *Autorité* will look at the answers competition law can provide (V), before proposing other responses to market failures (VI). The final section will be devoted to future prospects (VII). A glossary is appended to this opinion.

11. As the cloud is by its very nature a highly dynamic sector, the analysis proposed by the *Autorité* in this opinion is an assessment of the operation of competition in this sector on the date of its publication, and is likely to evolve.

[16] See glossary and developments below.

I. The cloud sector

A. CLOUD SERVICES

1. WHAT IS THE CLOUD?

12. The cloud is defined by the U.S. *National Institute of Standards and Technology* (hereinafter "NIST"[17]) as "*a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*."[18] They offer the possibility to outsource "*the management of all or part of the existing software, applications and IT services*"[19].

13. Traditionally, companies had to set up and manage an IT system tailored to their needs, involving time-consuming and costly infrastructure procurement processes (physical servers, data centres, hardware, etc.) and IT staff capable of maintaining, operating and upgrading this IT system on site. These processes could be managed in-house or outsourced to specialist companies. New Internet and computer technologies have opened up new possibilities, enabling - with the cloud - the use of remote computer servers to store data, access software or mobilise computing power.

14. The rise of this new approach to computing was made possible by the advent of virtualisation[20] in the late 1990s, with companies such as VMware making it possible to run several applications or operating systems on a single physical server. This technology made it possible to share and optimise infrastructures, improving companies' ability to access IT resources tailored to their current needs, at lower cost. Many companies have taken advantage of these new opportunities for their own activities.

15. The development of the cloud has taken on a new dimension with the provision of IT services to a wider customer base, pooling resources between several companies and developers. Having acquired extensive experience and developed a large-scale IT architecture for its Amazon.com service, capable of absorbing peaks in activity (particularly during sales periods), in 2006 Amazon decided to make this architecture available to other companies. In this way, it has enabled them to exploit unused computing capacity on its servers during periods of lesser activity. Amazon provides these services through Amazon Web Services (hereinafter "AWS"). AWS reports that it has thus offered a suite of IT services that are "*on-*

[17] The National Institute of Standards and Technology is a unit of the U.S. Department of Commerce. Its main mission is to develop and promote standards to facilitate innovation.

[18] NIST, 2011: ‘.

[19] Autorité de la concurrence, Opinion 21-A-05 of 29 April 2021 on the sector of new technologies applied to payments.

[20] Virtualisation consists of partitioning a computer or physical server into several virtual machines. Each virtual machine can then act independently and run different operating systems or applications while sharing the resources of a single host computer (Microsoft Azure, "What is virtualization?", link).

demand, scalable [[21]] *and modular* [*delivered*] *over the Internet and* [*offered*] *on a pay-per-use basis*".

16. This type of service has since been developed and has been taken up by several providers, leading to the deployment of the public cloud[22]. Public cloud services are provided by a third party, accessible *via* the Internet and adaptable to demand. Cloud services can also be deployed *via* a private cloud or a hybrid cloud. A private cloud is an infrastructure dedicated to a single organisation, which can be managed internally or externally (by a third party) and is usually hosted locally. A hybrid cloud is a combination of private and public cloud services. For example, it allows a company to store sensitive data in a private cloud and still benefit from the sharing and on-demand capabilities of the public cloud.

17. This opinion focuses mainly on the public cloud, which enables IT resources to be shared in an elastic manner and optimises the cost of these resources for companies by pooling them across different usage profiles. The private cloud, dedicated to a single organisation, is less elastic than the public cloud, as it is limited by the private resources available, particularly in the event of rapid and significant scalability, and is closer to traditional corporate IT systems.

18. The public cloud offers many advantages for companies. In particular, it gives them fast, easy access to IT resources that they no longer need to procure, configure or manage themselves. This limits the need for in-house IT staff and refocuses their resources on their core business. They can also use a self-service consumption model, with costs linked to what has actually been used. They therefore move from a fixed-cost model, having to invest in their necessary resources, to a variable-cost model based on usage. The ability to adjust production capacity to business demand is a particularly attractive asset for growing companies. It means that they can free themselves from the investment that would otherwise have been necessary for them to have their own resources to meet their changing needs.

19. Furthermore, by using specialised cloud service providers who invest in the development of these shared services, companies can easily access a wide range of services and the latest innovations. The public cloud also encourages the emergence of innovative services.

20. In addition, the public cloud gives companies new ways of organising work, based on shared, remotely-accessible resources, which can be a source of productivity gains. The crisis linked to the Covid-19 pandemic underlined even more clearly the usefulness of this technology and its contribution to business resilience, leading to an acceleration in investments by companies and administrations. In 2017, a study commissioned by the Commission estimated that the widespread adoption of cloud services would boost European GDP by 449 billion euros[23].

21. As a result of these advantages and the multiplication of uses, the public cloud has seen strong growth in recent years, and this is set to continue[24].

22. Lastly, it is clear from the information collected during the course of the investigation that the public cloud is seen as the model destined to become dominant in the future, while the

[21] In IT, "scalability" refers to the ability to resize capacity according to demand.

[22] See glossary.

[23] Deloitte, "Measuring the economic impact of cloud computing in Europe", 10 January 2017 (link).

[24] Gartner, “Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021”, 21 April 2022 (link).

private cloud is seen more as a transitional model or one designed for certain specific uses. This trend can already be seen, with turnover growth generated by the public cloud in France estimated at 35% between 2020 and 2021, compared with 5.7% for the private cloud[25].

2. The different cloud services

23. The public cloud generally comprises commercial offerings that give customers direct access to a large number of services. NIST distinguishes three main categories of cloud services: IaaS ("Infrastructure-as-a-Service"[26]), PaaS ("Platform-as-a-Service"[27]) and SaaS ("Software-as-a-Service"[28]). Whether a service belongs to a model depends on the degree of outsourcing of the service in question (as explained in figure 1 below):

- IaaS corresponds to the least outsourced model, in which the supplier provides the user with IT infrastructure, such as servers, networks, storage and data centre space. NIST defines this term as "*the capability* [...] *to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls)*" [29];
- PaaS 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. These environments include database and data analysis tools. NIST defines this term as follows: "*the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment*"[30];
- SaaS is the most outsourced model. It gives users direct access to applications, managed entirely by the supplier, from any connected device. NIST defines this term as follows: "*the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a programme interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating*

[25] Markess by Exaegis - Competitive environment - Digital infrastructures and Cloud 2022 strategies.

[26] IT infrastructure as a Service. See glossary.

[27] Platforms as a Service. See glossary.

[28] Software as a Service. See glossary.

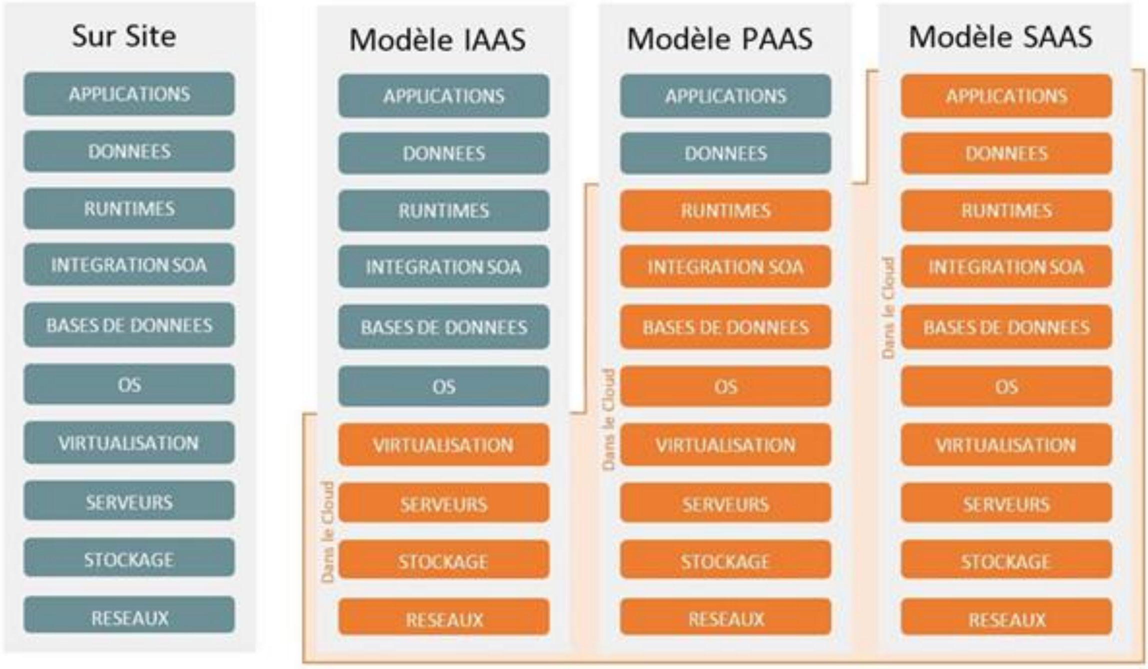
[29] Definition taken from the NIST website.

[30] Definition taken from the NIST website.

systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings"[31].

[31] Definition taken from the NIST website.

Figure 1 - Breakdown of responsibilities by cloud model[32]



Source: Atys Concept (link)[33].

FR	ENG
Sur Site	On website
Modèle IAAS	IAAS model
Modèle PAAS	PAAS model
Modèle SAAS	SAAS model
Applications	Applications
Données	Data
Runtimes	Runtimes
Intégration soa	Soa integration
Bases de données	Databases
OS	OS
Virtualisation	Virtualisation
Serveurs	Servers
Stockage	Storage
Réseaux	Networks
Dans le Cloud	In the Cloud

24. The information collected during the investigation tends to show that the IaaS and PaaS models are quite distinct from the SaaS model. The customers, uses and business models

[32] OS: Operating System (e.g. Windows); SOA integration: SOA stands for "Service Oriented Architecture".

[33] The "*on-premise*" column corresponds to the traditional IT model, in which the company's entire information system is hosted on its physical site.

appear to be very different. Services belonging to the IaaS and PaaS models are mainly aimed for IT professionals to build solutions for their own internal and/or external use. These services are also offered on a pay-per-use basis. The SaaS model, on the other hand, is mainly distributed to software end-customers on a subscription basis. Furthermore, while IaaS and PaaS providers are largely the same, they are more distinct from SaaS providers. There are more SaaS providers than IaaS and PaaS providers, and most SaaS providers come from the software world.

25. In line with the approach proposed in the aforementioned public consultation, the *Autorité* has therefore decided to focus primarily on IaaS and PaaS services in this opinion, although certain developments may, where appropriate, consider the SaaS model.

26. As far as the IaaS and PaaS models are concerned, the investigation showed that they provide a useful classification for describing various major cloud services and for quickly identifying which cloud services correspond to customer's needs. This distinction is also used by the majority of players and by the authorities who have studied the sector. Over 86% of the customers who participated in the online survey said they referred to it within their company. However, this classification does not always ensure a satisfactory delineation between the multiple services. A number of players pointed out that the boundaries between IaaS and PaaS can be blurred, and are tending to fade. Depending on the provider, certain services may be considered as belonging to one or other of these models, and classifications may evolve over time as catalogues are enhanced. Similarly, some of the marketed services may combine IaaS and PaaS services.

27. Despite these limitations, for the remainder of the analysis, the main services offered by providers have been described, with a proposed classification based on the IaaS and PaaS models. This classification is indicative and has no bearing on the analysis of relevant markets in the cloud sector (see "Analysis of relevant markets in the cloud sector" developments below). It is neither intended to be exhaustive nor to constitute a strict categorisation, as several services may appear in more than one category.

a) IaaS

28. The information collected from industry players allows three main categories of IaaS services to be distinguished:

- **computing**: computing encompasses all services offering the capacity to process large amounts of information at the same time. This category includes virtual machines[34] and their architectures, graphics processing units (GPUs)[35] and scalability. For example, some services, offer an automatically resizable computing capacity.

Figure 2 - Examples of computing services from different providers[36]

[34] A virtual machine is an isolated and stand-alone software environment that simulates a physical computer. It enables several independent instances of operating systems and applications to be run on a single physical computer.

[35] A graphics processing unit (GPU) is a processor composed of numerous specialised cores. It enables image computation functions to be performed in parallel. It is generally found on graphics cards.

[36] The services listed in this and the following tables are not equivalent to each other, but they all fall into the same category of services.

Cloud service providers	Examples of computing services
AWS	Amazon Elastic Compute Cloud (EC2)
Google Cloud	Google Compute Engine
Microsoft Azure	Azure Compute
OVHcloud	Metal Instances
3DS Outscale	Flexible Computing Unit
Scaleway	Play 2 Instances

- **storage**: storage comprises all services enabling large volumes of data to be stored on remote servers via the Internet. This category includes the storage of "objects"[37], files or blocks[38], tools to assist data migration or transfer, as well as back-up copies and instant back-ups. For example, some service enable all types of objects and volumes of data to be stored and retrieved immediately.

Figure 3 - Examples of storage services from different providers

Cloud service providers	Examples of storage services
AWS	Simple Storage Services (S3)
Google Cloud	Cloud Storage
Microsoft Azure	Azure Blob Storage
OVHcloud	Object Storage
3DS Outscale	Outscale Object Storage
Scaleway	Object Storage

- **network**: a computer network is a grouping of two or more devices enabling data exchange and the sharing of common resources[39]. These devices use common rules, called communication protocols, to transfer information. For example, DNS ("Domain Name System") is a widely used cloud network service. It can be used to determine the IP address[40] associated with a domain name in a reliable manner and with low latency, which means with minimal delay for data transmission.

Figure 4 - Examples of network services from different providers

Cloud service providers	Examples of network services
AWS	Amazon Route 53

[37] Object storage is a storage technology in which data is divided into "objects" and stored in a single repository. These "objects" also contain the associated metadata. For example, it is widely used to store unstructured data (images, audio, video, etc.).

[38] Block storage is a technology that is used to break up data into blocks of restricted size and stored in such a way as to optimise its availability.

[39] https://www.ionos.fr/digitalguide/serveur/know-how/reseau-informatique-definition/.

[40] The IP (Internet Protocol) address is a unique identification number associated with any peripheral device connected to the computer network.

Google Cloud	Google Cloud CDN
Microsoft Azure	Azure Virtual Network
OVHcloud	OVH Floating IP
3DS Outscale	Outscale DirectLink
Scaleway	Private Network

29. IaaS services represent, in terms of numbers, a small proportion of all public cloud services, not least due to the growing diversity of PaaS services (see below). However, they still account for the vast majority of cloud services business and revenues, with IaaS services providing the essential foundation on which companies can build their cloud architecture.

30. IaaS services are the most standardised of all cloud services. Several players in the sector refer to this as a "*commodity*". These services are provided uniformly by all cloud service providers, although there may be variations in terms of invoicing or service guarantees.

b) PaaS

31. PaaS covers a wider range of services than IaaS. In addition, their number is constantly increasing given the high degree of innovation, which complicates the categorisation of its different services. This means that any attempt to categorize is necessarily incomplete, with overlaps between categories.

32. Based on the information collected, the *Autorité* proposes to distinguish the main PaaS services into the following broad categories:

- **databases**: a database is a repository of information, which may or may not be structured[41]. A cloud database (also known as "DBaaS" for "DataBase-as-a-Service") is a database running on the cloud provider's IT infrastructure, which the customer accesses *via* the Internet. There are two main categories of database:

    i. **relational databases** are a set of interdependent tables where information is organised in rows and columns. The relationship between information is specified in a diagram. These databases are generally written in a structured language, with SQL (Structured Query Language) being the most popular. Cloud service providers offer systems for managing these databases, either distributed under licence, such as Microsoft's Azure SQL Database service or Oracle, or available as open source, such as MySQL or PostgreSQL;

    ii. **non-relational databases** do not use table models. Their contents are stored in a single document. Since they are unstructured, these databases are also sometimes referred to as NoSQL. Cloud service providers also offer tools for managing this data, such as AWS with Amazon DynamoDB and Microsoft with Azure Cosmos DB.

[41] Structured data is data that uses a predefined and expected format (Oracle, "Comparison between structured and unstructured data types", link).

Figure 5 - Examples of database services from different providers

Cloud service providers	Examples of database services
AWS	Amazon Aurora
Google Cloud	Google Cloud Bigtable
Microsoft Azure	Azure Cosmos DB, Azure SQL DB
OVHcloud	OVH Managed Databases for PostgreSQL
Scaleway	Managed Database for Redis

- **data analysis**: the leading cloud service providers offer tools for processing and analysing large volumes of data. These tools can perform queries[42] on (structured or unstructured) data stored in the cloud, store and manage data in data lakes[43], or enable the optimised deployment of computer clusters (e.g. Apache Spark[44]);[45]
- **tools for developers**: refers to all the tools used to develop applications in the cloud, such as integrated development environments and software development kits;
- **artificial intelligence and/or machine learning tools**: such as machine learning platforms, natural language processing tools and image and video content processing tools;

Figure 6 - Examples of machine learning services from different providers

Cloud service providers	Examples of machine learning services
AWS	Amazon Augmented AI
Google Cloud	Google Text-to-Speech
Microsoft Azure	Azure Cognitive Services
OVHcloud	OVHcloud AI training
Scaleway	Machine Learning Images

- **services required to operate the Internet of Things**[46]: these services enable connected devices to be connected and managed, and the data collected from them to be collected, stored and analysed;
- **IT containers**: in IT, a container is a single software package containing the code for an application, together with all the elements required to run it. This technology

[42] In computing, a query is a request to a database. It may contain a number of criteria to help refine it.

[43] A data lake contains unstructured data. There is no hierarchy or organisation between the different data elements. The data is stored in its most raw form and is not processed or analysed. A data lake accepts and stores all the data from different sources and supports all data types (Oracle, "Data Lake: Definition", link).

[44] Apache Spark is an open-source environment for distributed computing, i.e. optimised for processing very large volumes of data.

[45] According to www.lebigdata.fr: "*A server cluster is a group of servers and other independent resources operating as a single system*", link.

[46] The Internet of Things refers both to the process of connecting physical objects to the Internet and to the network that connects these objects (OVHcloud, What is the Internet of Things? link).

enables developers to deploy their applications independently of the cloud environment. The automation of deployment and the scaling and management of these containers are carried out by a container orchestrator, with Kubernetes being the most widely used. Kubernetes is a system initially developed by Google, then made *open source* in 2014[47] and now hosted by the Cloud Native Computing Foundation (CNCF)[48]. Most cloud service providers use this technology to deliver PaaS services such as Scaleway's Kubernetes Kapsule or Google Cloud's Google Kubernetes Engine. The categorisation of containers within PaaS can be open to discussion, since they contain infrastructure services, unlike other PaaS services. Some players refer to this as CaaS (Container-as-a-Service)[49];

- **security** ("Security, Identity and Compliance"): security refers to all the cloud services designed to secure the use of the cloud by companies. It includes firewall[50], identity management, data protection, network protection and vulnerability detection services. By way of illustration, Identity and Access Management (IAM) services manage the authorisations for individuals to access functions. For example, Microsoft's cloud-based service Azure Active Directory (Azure AD) is used very often[51]. These services are used at all levels of cloud services, and it is difficult to classify them precisely as PaaS or IaaS.

33. PaaS services are becoming increasingly diversified and represent a growing proportion of the public cloud services offered to companies. As an example, Google Cloud Platform offers more than a hundred services, and of the 12 "characteristic products" mentioned on its site[52], eight are PaaS services, according to the typology described above. In this highly innovative environment, services vary from one provider to another.

[47] More information on Kubernetes online (link).

[48] More information on the CNCF online (link).

[49] See proposed illustration (link).

[50] A firewall is a product that forms a protective barrier between a computer network (in this case, the cloud service provider's network) and the outside world. In particular, it filters out malicious traffic and attacks.

[51] https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whatis.

[52] Selection of products (Compute Engine, Cloud Storage, BigQuery, Cloud SDK, Cloud SQL, Google Kubernetes Engine, Cloud CDN, Dataflow, Operations, Cloud Run, Anthos, Cloud Functions) presented on the GCP website (link).

Cloud services

The public cloud generally comprises commercial offerings that give customers direct access to a large number of services. There are three main categories of cloud services: IaaS, PaaS and SaaS:

- IaaS corresponds to the least outsourced model, in which the supplier provides the user with IT infrastructure, such as servers and storage;
- PaaS 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 typically associated with the process;
- SaaS is the most outsourced model. It gives users direct access to applications, managed entirely by the supplier, from any connected device.

These three broad categories correspond to different levels of responsibility devolved between the cloud service supplier and the customer company. Whether a service belongs to a model depends on the degree of outsourcing of the service in question.

The IaaS and PaaS models are quite distinct from the SaaS model. The customers, uses and business models appear to 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 uses.

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. PaaS services are very diverse.

B. USE OF CLOUD SERVICES

1. CLOUD SERVICE CUSTOMERS

34. This opinion focuses on business customers, who are the main users of IaaS and PaaS services. The end customers can be developers or companies with IT resource requirements. It should be noted that cloud service suppliers can also provide services to resellers and partners on a "white label" basis. The latter then market these solutions to their customers under their own brand name.

35. Companies face a variety of IT needs in the course of their business. Different software and services may be required to enable companies to create the right IT solutions for every need. Each solution can be referred to as a "workload", which corresponds to the set of IT resources (such as applications, data and services) or business processes that meet a specific need or objective. In its response to the public consultation, one provider defined workloads as "*made up of a set of customer applications, components and associated data that can be considered as meeting a specific objective or constituting a management unit, from the customer's point of view. These applications, components and data interact with each other horizontally and vertically, passing through different elements within the cloud to serve a particular function.*"[53]

[53] The above-mentioned public consultation document gave examples of workloads, such as an e-commerce site workload based on several cloud services (a content delivery network (CDN) service combined with an object storage service for the static content layer, an API management service for API design and management, a customer identity and access management (CIAM) service for the authentication layer, and a serverless event computing service (FaaS) combined with an indexed NoSQL database service for the dynamic content layer).

36. Cloud service customers have chosen to use these services for some or all of their workloads. Among them, it is particularly interesting to distinguish different categories of players according to their stage of adoption of the cloud. In particular, it is possible to distinguish between customers with IT solutions historically hosted and managed on-premise who are gradually migrating all or part of their workloads to the cloud (a) and those who have developed their IT solutions directly from cloud services, commonly referred to as "cloud native" (b). Customers can also be distinguished by sector (c) or size (d).

a) Companies migrating to the cloud

37. Many companies have workloads designed to run on-premise and may decide to upgrade their IT systems by migrating all or part of their workloads to the cloud if relevant given its advantages.

38. In this case, companies are faced with specific issues in relation to adapting their workloads to operate under a cloud model and managing the parallel operation between their on-premise and cloud-hosted solutions (see Part IV). As a result, these companies experience transition periods of varying lengths depending on the number and size of the workloads they decide to migrate. The information collected during the investigation shows that many companies are experiencing migration processes lasting more than two years.

39. Migrating a workload can also be very costly, especially for large companies with complex on-premise information systems. The *Autorité* found a wide range of migration costs in the responses to its online survey, mainly due to the variety of company sizes and workloads. The median cloud migration cost reported by respondents was over 450,000 euros, while the average was around 6.6 million euros. Some 44% of respondents said they had used the services of an integrator to facilitate this migration. Some cloud service providers also offer their own migration support services.

40. The vast majority of companies (87% of online survey respondents) that have migrated to the cloud have adopted a public or hybrid cloud deployment.

41. These companies are prime targets for cloud service providers, as their migration process is relatively recent and in progress. Suppliers can position themselves as primary providers and offer services for the part of the workloads that have yet to be migrated to the cloud as part of a so-called multi-cloud strategy (see 4. Multi-cloud). Given the recent nature of this migration (see 2. Cloud adoption by French companies) and its high costs (see Part IV), companies migrating from one cloud service provider to another are still rare but could become more frequent over the next few years. Similarly, it should be noted that migrating to the cloud is - at least in the medium term - an irreversible decision for a company, as a return to on-premise operation would entail irrecoverable costs. However, companies can opt for a hybrid strategy that combines in particular public and private clouds.

b) Cloud natives

42. In contrast to companies migrating to the cloud, 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 companies therefore do not have to transform their IT systems in order to migrate to the cloud. Many cloud-native startups have benefited from the flexibility and resizing of their resources made possible by the cloud. Over the past few years, this category of customers has been a prime target for cloud service providers, due to

their interest in cloud services, their often data-driven operation and their rapid ability to adopt these new tools with no history to adapt.

43. In addition to the creation of new cloud-native companies, these companies have now already chosen one or more providers. The choice of provider(s) with which to build their IT system is key for their further development. Just like other corporate cloud service customers, cloud-native companies will therefore be prime targets for providers, mainly as part of the development of a multi-cloud strategy or the decision to migrate to another provider.

c) Customers by sector

44. Today, business customers for cloud services cover all sectors including industry, energy, construction, trade, transportation, accommodation and food service activities, information and communication, financial services, government, education, healthcare and other service activities. However, there may be differences in usage or maturity in migrating to the cloud, depending on the sector.

45. Certain highly regulated sectors such as the public sector, operators of essential services (hereinafter "OESs"[54]) and operators of vital importance (hereinafter referred to as "OVIs"[55]), financial services and healthcare for example, have to comply with certain constraints that may affect their use of the public cloud. The regulatory framework for data protection (see box), which is mostly subject to legal uncertainties, is also helping to define new rules, particularly for certain sensitive sectors of activity.

An uncertain data protection framework

The process of the corporate adoption of cloud services is taking place in the context of the existing fragility of the data protection frameworks which raises issues of sovereignty. The "Schrems II" judgment[56], issued by the Court of Justice of the European Union (CJEU) on 16 July 2020, invalidated the system of data transfers between the European Union and the United States[57] ("Privacy Shield")[58]. This ruling raises questions about the extent of the legal

[54] ANSSI defines an OES as follows: "*An OES is an operator dependent on information systems or networks, providing an essential service whose interruption would have a significant impact on the functioning of the economy or society. An essential service meets three criteria: this service is essential to the maintenance of critical societal or economic activities; the provision of this service is dependent on information systems or networks; an incident on these networks and systems would have a significant disruptive effect on the provision of said service*" (link).

[55] OVIs are designated by law as having activities essential to the survival of the nation or dangerous for the population. The sectors of vital importance include the civil and military activities of the State. The list of OVIs is classified as "secret defence" (see Article R.1332-2 of the French Defence Code (Code de la défense).

[56] CJEU, judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559.

[57] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield (OJEU L 207 of 1 August 2016, pages 1-112).

[58]According to the Court, the restrictions on the protection of personal data which derive from the United States' domestic regulations (Cloud Act) on access to and use by the United States public authorities of such data transferred from the European Union to that third country are not regulated in a way that meets requirements that are substantially equivalent to those required under European Union law by the principle of proportionality,

risks associated with the application of non-European laws to French and European customers and cloud service providers. Following the announcement by the European Union and the United States of a new political agreement on 25 March 2022[59], the President of the United States signed a Decree on 7 October 2022, implementing this agreement in principle in US law. The Commission published a draft adequacy decision on 13 December 2022, before launching the adoption procedure[60]. Pending the outcome of this procedure, this situation of uncertainty and the regulatory requirements in some sectors (see below) are prompting authorities and certain players to develop solutions that guarantee the protection of sensitive data at European level, as demonstrated by the various security certifications developed below.

inasmuch as the surveillance programmes based on those regulations are not limited to what is strictly necessary.

[59] European Commission press release, "*European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework*", 25 March 2022 (link).

[60] Commission press release, "*Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US*", 13 December 2022 (link).

The public sector

46. In France, the public sector stands out from other sectors due to the specific doctrine on the use of cloud services. As part of its national cloud strategy[61], the French government has defined, among other things, the "cloud at the centre" doctrine for the State's digital transformation.[62] This doctrine applies to State stakeholders and organisations under its supervision, as selected in Decree 2019-1088 of 25 October 2019 defining the State information system[63]. The cloud will now be the default hosting and production mode for the French government's digital services, for all new digital products and for products undergoing substantial evolution. As a result, for all new projects, the French government's IT teams and their service providers must by default use one or more in-house or commercial cloud offerings to cover the entire application production cycle, based on criteria such as the required level of security.

47. In this context, if a public-sector IT system or application uses particularly sensitive data[64], it will have to use the State's internal cloud or private providers certified as SecNumCloud by the *Agence Nationale de la Sécurité des Systèmes d'Information* (French National Cybersecurity Agency, hereinafter "ANSSI") and protected against all non-EU regulations[65].

48. This doctrine constrains the demand from government bodies for cloud services, particularly those using particularly sensitive data.

SecNumCloud certification

As the national authority for the security and defence of information systems, ANSSI grants security authorisations to solutions, products or services that demonstrate a high level of security and trust. As part of this approach, in 2016 the Agency drew up the SecNumCloud repository[66] to enable the qualification of cloud computing service providers. The key requirements of the repository include:

- compartmentalisation of flows between operations linked to the proper functioning of the qualified service and those linked to the use of the service by entities using a cloud computing service provider. This translates into network isolation requirements to guarantee compartmentalisation between the different components of the cloud service: cloud usage, service management, infrastructure management, etc. A further requirement is that the administration interfaces used by the service provider and those made available to customers must be separated and protected (chapters 9.6 and 13.2 of the requirements);

[61] See the Cloud doctrine at the centre of Circular 6282-SG of 5 July 2021 on the doctrine for the use of cloud computing by the State (link).

[62] See the "National Cloud Strategy" press kit (link).

[63] Decree 2019-1088 of 25 October 2019 on the State's information and communication system and the interministerial digital directorate.

[64] Circular 6282-SG specifies that "*if the IT system or application handles particularly sensitive data, such as the personal data of French citizens, economic data relating to French companies, or business applications relating to government employees, the commercial offer selected must comply with SecNumCloud qualification (or a European qualification of at least equivalent level), and be immune to all extra-Community regulations,*" pages 10-11.

[65] Press release from the Ministry of Transformation and the Civil Service, "*The State specifies the implementation of the "cloud at the centre" doctrine*", 6 October 2021 (link).

[66] Cloud computing service providers (SecNumCloud) - requirements framework, Version 3.2 of 8 March 2022.

- protection of workstations used to administer the SecNumCloud-qualified service (chapter 12 of the requirements);

- additional requirements for data localisation within the EU. These requirements concern data storage and processing, as well as service administration and supervision operations (chapter 19.2. of the requirements);

- protection against non-European laws (chapter 19.6 of the requirements). From a practical point of view, this involves requirements relating to the location of the head office (established within an EU Member State), shareholding (third-party entities located in a non-EU State remain in the minority), control of the use of the services of non-EU third-party companies in terms of their ability to obtain the data collected through the SecNumCloud service, ongoing operating autonomy in the provision of the SecNumCloud service, and compliance with current legislation and the fundamental rights and values of the European Union. SecNumCloud version 3.2 goes further, guaranteeing that the cloud service provider and the data it processes cannot be subject to non-European laws. It also incorporates feedback from the first assessments and specifies the requirement to implement penetration tests throughout the qualification lifecycle.

Other similar certifications have been developed in parallel in several European countries (ENS[67] in Spain, C5[68] in Germany, etc.). To avoid the fragmentation of the European market, the "Cybersecurity Act"[69], adopted in 2019, plans to harmonise these certifications through the creation of the EUCS (European Cybersecurity Certification Scheme for Cloud Services) scheme. This scheme is currently under discussion within ENISA, the European Union Agency for Cybersecurity. This certification should guarantee a very high level of cybersecurity for a service but also reward the localisation and processing of data hosted in the EU, as well as guaranteeing immunity with regard to the extraterritoriality of foreign laws. This last criterion is the main centre of debates between Member States.

OESs and OVIs

49. The activities of certain companies are considered essential to maintaining economic and social activity ("OES") or of vital importance ("OVI"). As a result, these companies must meet enhanced cybersecurity risk management obligations, set out in a number of regulatory frameworks.

The regulatory framework for cybersecurity

Cross-cutting cybersecurity legislation sets out the framework and obligations for cloud service providers, among others. Directive (EU) 2016/1148 "*Network Internet Security*",

[67] *Esquema Nacional de Seguridad* drawn up by the *Entidad Nacional de Acreditación* (ENAC).

[68] *Cloud Computing Compliance Controls Catalog*, a standard that establishes a mandatory minimum baseline for *cloud* security and the adoption of public *cloud* solutions by German government agencies and companies working with the government.

[69] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act) (OJEU L 151 of 7 June 2019, pages 15-69).

known as "NIS"[70], adopted on 6 July 2016, has notably defined several obligations aimed at strengthening the cybersecurity of digital service providers, including cloud companies. This text was revised very recently by the "NIS2" Directive, which was adopted by the Council of the European Union on 28 November 2022[71] and came into force on 16 January 2023. Member States have 21 months to transpose the directive into national law.

50. Following the introduction of the NIS Directive, France set up a mechanism for identifying and designating ESOs[72], as well as a process for ANSSI to support these players in implementing cybersecurity frameworks to ensure their protection. The NIS2 Directive strengthens the governance and management of digital risk for OESs and increases the security of the digital ecosystem (subcontractors, providers, and partners) around them. The scope of the targeted sectors and activities has also been broadened and should give rise to a significant increase in the number of designated OES players. This regulatory framework may lead to particular demands from OESs in their choice of information system and provider.

51. The French Military Programming Act of 18 December 2013 also introduced a system to protect OVIs[73]. The cybersecurity component of this law created specific provisions for the security of information systems in the French Defence Code (*Code de la défense*), notably requiring OVIs to strengthen the security of critical information systems[74] (SIVIs). In particular, OVIs must take the necessary measures, including by contracts, to guarantee the application of security rules for the SIVIs set up by their subcontractors. SIVIs must be certified, which requires audits to be carried out either in-house or by a service provider selected by ANSSI. All these specific rules have an impact on OVIs' demand for IT units, particularly cloud services.

52. With its "cloud at the centre" doctrine, the French government has also demonstrated its determination to further direct demand from OESs and OVIs. The press kit on the government's cloud strategy states that: "[w]*hile the "cloud at the centre" doctrine applies to all ministries and their subordinate administrations, the government's intention is to set an example and encourage OVIs, OESs and local and regional public authorities to use the cloud and SecNumCloud offers for sensitive data*"[75].

[70] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJEU L 194 of 19 July 2016, pages 1-30).

[71] Council of the European Union, "*EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation*", 28 November 2022 (link).

[72] Based on the list of essential services set by decree, ANSSI, in coordination with the ministries, proposed a list of potential OESs to the Prime Minister. Following inter partes proceedings, the Prime Minister designates the OESs by means of a designation decree. Further information is available on the ANSSI website (link).

[73] Act 2013-1168 of 18 December 2013 on Military Programming for 2014 to 2019 and on various provisions concerning defence and national security, Official Journal of the French Republic (JORF) 0294 of 19 December 2013.

[74] According to ANSSI, critical information systems are *"systems whose security or operation would be compromised in such a way as to significantly diminish the war or economic potential, security or survival capability of the Nation"*.

[75] National Cloud Strategy, "Supporting innovation in the Cloud", press kit, 2 November 2021, page 26 (link).

Financial Services

53. Cloud service customers in the financial sector represent a particular profile that influences demand, whether in terms of security guarantees, the ability to evaluate their providers or the use of multi-cloud.

54. In the financial sector, national and European banking and financial market regulators have been looking for several years at the issues raised by the use of outsourced Software vendors, given the specific risks associated with financial activities. This has given rise to several reports such as the one by the *Autorité de Contrôle Prudentiel et de Résolution* (ACPR) on *The risks associated with Cloud computing*[76] in July 2013 or the one published in May 2021 by the *Haut Comité Juridique de la Place Financière de Paris* (HCJP) on the cloud banking[77].

55. To help financial institutions identify, manage and monitor the risks arising from the use of the cloud, national and European banking and financial market regulators have drawn up a number of recommendations. In 2019, the European Banking Authority (hereinafter "EBA") published its *Guidelines on outsourcing arrangements*[78] on the management of information technology and security risks for financial institutions. While most national supervisory authorities have declared their compliance with these Guidelines, the regulatory framework in the different Member States governing the use of the cloud by banking and financial institutions has appeared heterogeneous and insufficient in relation to the growing role of IT service providers and cloud services in particular.

56. Specifically, financial regulators have highlighted the financial sector's growing dependence on a small number of cloud providers. A joint report published on 31 January 2022 by the three European regulators (the EBA, the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA)) thus warns of the risks of mergers in unregulated sectors such as the cloud.[79] Similarly, in July 2022, the Bank for International Settlements (BIS) published a report expressing its concerns at the growing dependence of financial institutions on a small number of providers capable of operational and security failures. The report also noted the reduced ability of these institutions, as well as regulatory authorities, to properly assess compliance and risk of using such providers due to the limitations introduced into contracts for the provision of cloud services, particularly with regard to the right to audit[80].

57. All these concerns have led to a tightening of the regulatory framework. The European DORA regulation ("*Digital Operational resilience of the financial sector*"[81]), adopted by the

[76] ACPR, The risks associated with Cloud computing, Analyses and Overviews, no. 16, July 2013 (link).

[77] HCJP, Report on the cloud banking: state of play and proposals, May 2021.

[78] EBA, Final report on Guidelines on outsourcing arrangements, 25 February 2019 (link).

[79] EBA, EIOPA, ESMA, *Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues*, 31 January 2022, paragraph 143 (link).

[80] BIS, *Big tech interdependencies - a key policy blind spot*, July 2022.

[81] European Commission, Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM/2020/595 final, 24 September 2020.

Council of the European Union on 28 November 2022[82], aims to strengthen the resilience of the financial sector with regard to cybersecurity risks in particular, and ensure better control in the sector over the outsourcing of their IT services. Its application, scheduled for 17 January 2025 at the latest, will require European regulators to develop regulatory technical standards for the technical implementation of the principles set out in the regulation. Article 5 of the regulation also calls for the implementation of a multi-cloud strategy to reduce dependency and increase the operational resilience of financial services.

Healthcare

58. In healthcare, companies must comply with a set of rules designed to protect the health data of individuals. This means that data must be hosted under appropriate security conditions. Article L. 1111-8 of the French Public Health Code (*Code de la santé publique*) stipulates that "*healthcare professionals or facilities, or the data subject, may deposit personal health data*" with "*healthcare data hosts*" ("HDS"), i.e. persons hosting personal health data "*collected or produced in the course of preventive, diagnostic or therapeutic activities*"[83]. These rules can lead customers in the healthcare sector to choose one provider over another, depending on whether or not its services are certified.

59. At European level, it is worth noting that the proposed regulation on the European Health Data Space[84], presented on 3 May 2022, also includes specific rules for data in the health sector. Once set up, the European Health Data Space should define a framework for sharing health-specific data, and establish infrastructures for the use of electronic health data across the European Union.

d) Customers by company size

60. Cloud service customers come in all sizes, from very small enterprises (hereafter, "VSEs") to large enterprises. Migration to the cloud concerns all categories, whether large enterprises, small and medium-sized enterprises (hereafter "SMEs"), very small businesses or public entities.

61. The information collected during the investigation shows that the criteria for choosing a cloud service provider tend to vary according to the size of the customer company. For VSEs/SMEs, the nationality (French or European) of the cloud service provider and its regulatory compliance (e.g. in the health sector) appear to be a particularly important criteria. Large enterprises seem to refer to more operational criteria such as service quality and availability, proximity to data centres (to reduce latency), international presence, and access to an ecosystem of other services or the provider's reputation. However, security concerns are equally important for both customer segments. Similarly, for both categories, the responses obtained tend to show that price is not the main criterion for choice, with priority given to the quality of the service provided.

[82] Council of the European Union, "*Digital finance: Council adopts Digital Operational Resilience Act*", 28 November 2022 (link).

[83] Article L. 1111-8 of the French Public Health Code (Code de la santé publique).

[84] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM (2022) 197 final, 3 May 2022.

2. Cloud adoption by French companies

62. Between 2014 and 2021, the percentage of companies with more than 10 employees, excluding the financial sector, indicating that they use cloud services (SaaS included) rose from 12% to 29% in France[85].

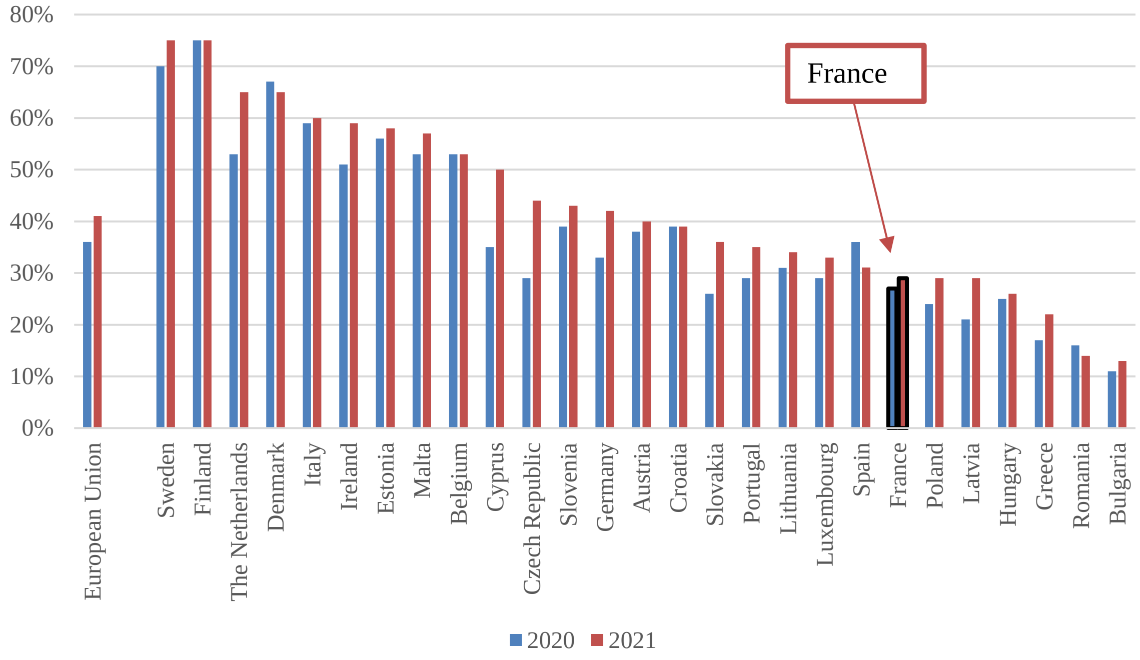
63. While not all French businesses will use cloud services, these figures point to significant growth potential. In Sweden and Finland, for example, the number of companies using cloud services was around 75% in 2021 (see Figure 7).

64. However, this migration has been slower in France than in the rest of Europe in recent years. Still during the 2014-2021 period, cloud adoption rose from 18% to 41% on average in the European Union. In France, while the trend is accelerating, with a 10% increase between 2018 and 2021, against the backdrop of the Covid-19 pandemic, this rise also remains lower than the average observed in European Union Member States (+17% over the same period)[86].

[85] Eurostat, use of cloud computing services.

[86] Eurostat, use of cloud computing services, 17 March 2022.

Figure 7 - Use of cloud services in 2020 and 2021 by EU Member State (% of companies)

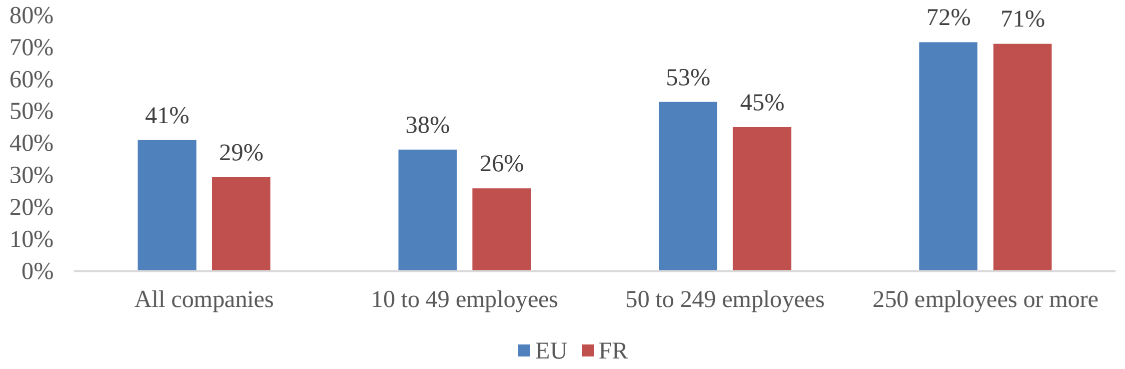


Source: Eurostat, "Cloud computing - statistics on the use by enterprises", December 2021 data (link).

65. France is lagging behind, with SMEs and VSEs migrating more slowly. In 2021, the cloud adoption rate among large enterprises was 71.6% in the European Union, and 71.1% in France for medium-sized and large enterprises (see Figure 8).

66. Some providers also believe that gaps in skills and digital maturity, as well as heightened concerns regarding data security and confidentiality, may explain the less mature French market. Many cloud service providers and customers also informed the *Autorité* that regulatory developments around cybersecurity, data protection and extraterritoriality may have created considerable uncertainty for some customers, causing them to reconsider or slow down their migration to the cloud.

Figure 8 - Comparison of cloud usage in France and the EU average in 2021 by company size (% of companies)



Source: Eurostat, "Cloud computing - services by size class of enterprise", December 2021 data (link).

A challenge for the digital transformation of the economy

The European cloud market could grow from 53 billion euros in 2020 to 560 billion euros in 2030, with average annual growth exceeding 25%[87].

This growth in the cloud is accompanied by significant government support in the research and development of innovative technologies, in order to support the digitisation of the economy as well as European and French industry. At European level, the Commission has asked Member States to devote at least 20% of the sums received under the 2020 European Recovery Plan to digital investments, particularly in the cloud.

Several European industrial initiatives concern this sector. In June 2020, France and Germany[88] formalised the joint "Gaia-X" project, aimed at developing a European data infrastructure that meets common requirements, notably in terms of data security, interoperability[89] and portability[90]. An Important Project of Common European Interest ("IPCEI") for new-generation cloud and edge computing[91] infrastructures and services is also being set up, with 12 Member States involved and almost 60 projects involving 180 European companies[92]. At national level, a plan to support the French cloud industry was presented on 2 November 2021, mobilising almost 1.8 billion euros in public and private funding[93].

3. USE OF CLOUD SERVICES

67. In France, among the businesses using cloud services (including SaaS) in 2021, the main uses are for document storage (76%) and email (67%) (see Figure 9). More than half of companies also use database hosting and management services (59%) or IT security services (51%). However, the use of an application development, testing and deployment platform is still limited (25%).

[87] KPMG report, "The European cloud: major challenges for Europe and five scenarios with major impacts by 2027-2030", April 2021.

[88] Its founding members include 11 German companies (including Deutsche Telekom, Siemens, Bosch) and 11 French companies (including Orange, OVHcloud, Atos, EDF). By early January 2021, Gaia-X had received 200 membership applications from companies and research organisations all over the world.

[89] See glossary.

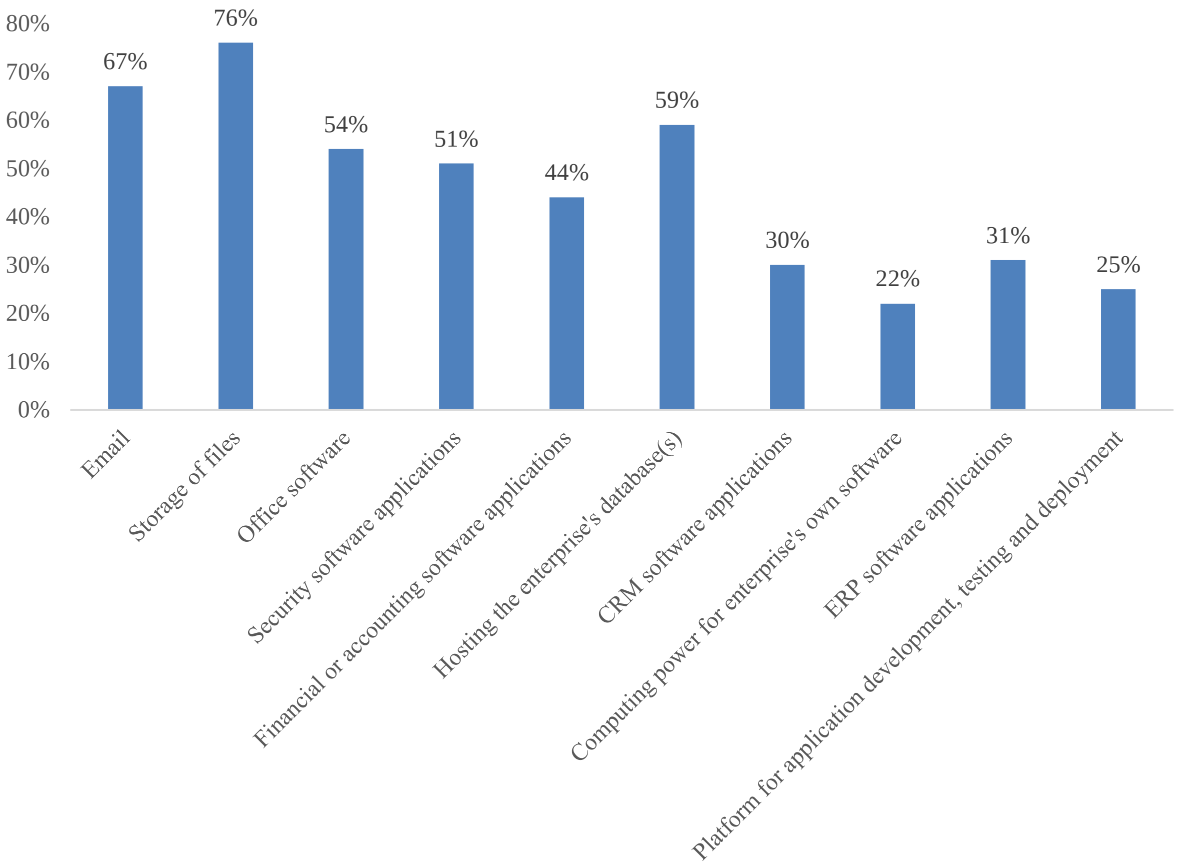
[90] See glossary.

[91] Edge computing" is defined as processing that takes place close to the data collection point.

[92] Press release, *"Bruno Le Maire and Jean-Noël Barrot reaffirm the national cloud strategy and announce new measures to support the sector"*, 12 September 2022 (link).

[93] See press release from the Government (link).

Figure 9 - Use of cloud services by businesses in 2021 in France (% of cloud users)

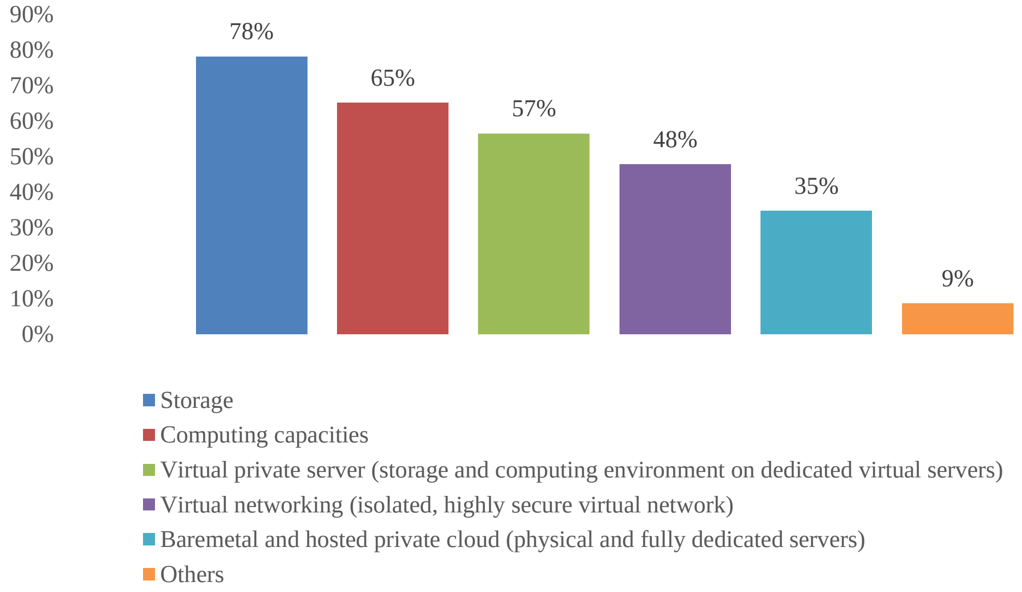


Source: Eurostat, Use of cloud computing services in enterprises, December 2021 data (link)

68. The data collected in the *Autorité's* online survey (see Figure 10) also shows that companies are making extensive use of IaaS services. Although these results are not statistically representative of the market, they are a useful illustration of the use of cloud services.

69. Of the 23 companies that responded to the survey, 78% said they used storage services. Storage and computing capacity services appear to be the most widely used, especially when compared with PaaS services (see below).

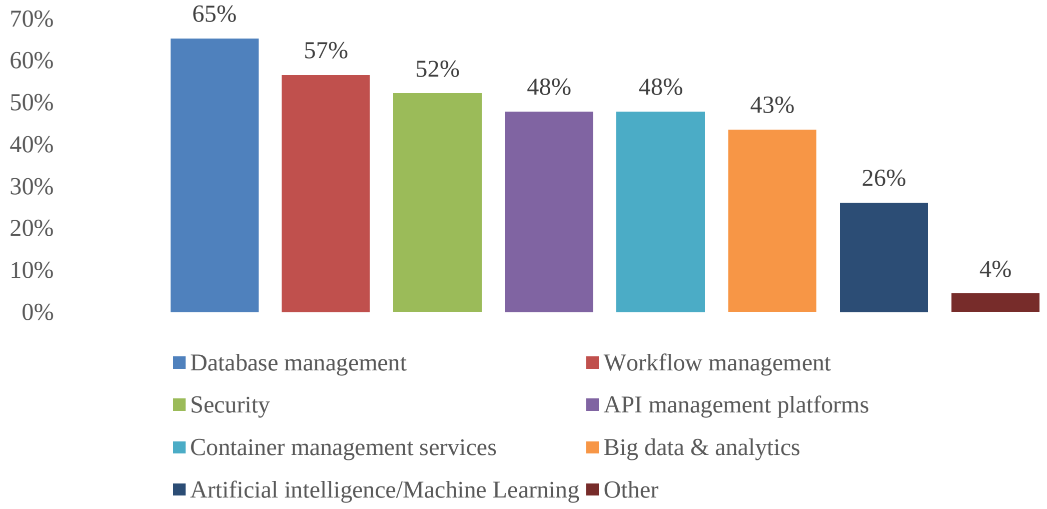
Figure 10 - Breakdown by category of IaaS services used by online survey respondents



Source: Online survey conducted by the Autorité.

70. Of the 23 companies that responded to the survey, a majority say they also use database management (65%), workflow management (57%) and security services (52%). More sophisticated artificial intelligence and machine learning services are still only used by a minority of PaaS users.

Figure 11 - Breakdown by category of PaaS services used by online survey respondents



Source: Online survey conducted by the Autorité.

4. MULTI-CLOUD

71. Multi-cloud is a term used by industry players to refer to the parallel use by a single company of services from multiple cloud service providers. This may involve using multiple providers for IaaS, PaaS or both (or even SaaS, depending on the definition). Many companies today seem to be implementing or wanting to implement a multi-cloud strategy. According to a 2020 Gartner[94] survey of public cloud users[95], 81% of respondents indicated that they used services from at least two providers.

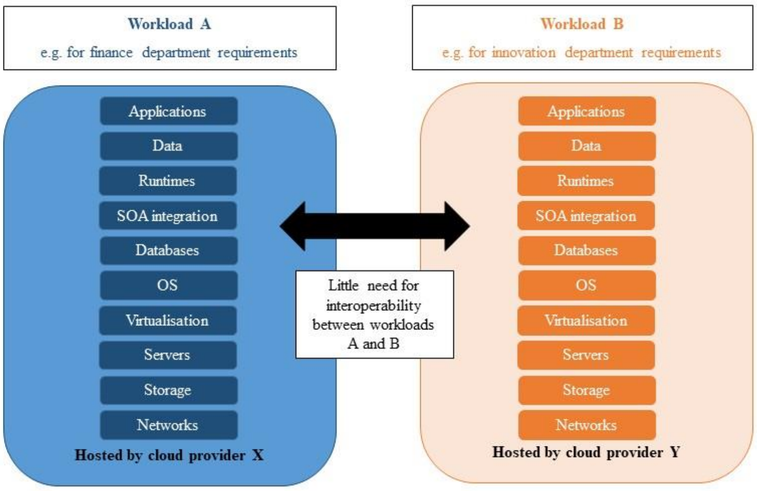
72. The information collected during the investigation also shows that companies very often use several cloud service providers for IaaS and PaaS services. For example, around 40% of respondents to the *Autorité's* online survey indicated that they use four or more IaaS and PaaS service providers.

73. However, the information collected tends to show that, even in the case of these multi-cloud strategies, companies generally only use one cloud service provider per workload. For a given workload, generally comprising several IT requirements, the company will choose the provider that appears to be the most suitable. In the end, the company may select several providers to provide services for different workloads, which may be managed by different business units, given the variable requirements from one workload to the other. These multi-cloud strategies are therefore more common in large companies, which have diverse and relatively independent internal needs and can choose to distribute them between different providers (see Figure 12).

[94] According to its financial report of 31 March 2023, Gartner "*delivers actionable, objective insights to executives and their teams*". It "*delivers its products and services through three business segments: Research, Conferences and Consulting*" (link).

[95] Gartner survey of public cloud users (link).

Figure 12 - Illustration of a multi-cloud strategy between different workloads


Workload A
e.g. for finance department requirements
Workload B
e.g. for innovation department requirements
Applications
Data
Runtimes
SOA integration
Databases
OS
Virtualisation
Servers
Storage
Networks
Hosted by cloud provider X
Applications
Data
Runtimes
SOA integration
Databases
OS
Virtualisation
Servers
Storage
Networks
Hosted by cloud provider Y
Little need for interoperability between workloads A and B

Source: Autorité de la concurrence

74. This situation can be explained by the fact that using several providers for the same workload raises technical difficulties, particularly with regard to interoperability requirements. For example, a company wanting to use one provider to host a database and another to use that data with an artificial intelligence service must guarantee strong interoperability between these services.

75. The investigation shows that multi-cloud strategies within a single workload are very rare among cloud service users. Most companies focus on the time, cost and technical investment required to achieve this. Indeed, the complexity of such projects, for example to ensure the necessary compliance with numerous regulatory standards, means that there is ultimately no return on investment.

76. Multi-homing[96] is also an underdeveloped strategy in the cloud, particularly due to the additional costs associated with duplicating the service, the complexity of mastering two solutions at the same time, and the increased risk of vulnerability to cyber-attacks (due to the increased number of targets).

[96] "*Multi-homing refers to a situation in which users tend to use several competing platform services in parallel*" and for the same data. European Commission, Study on *"Support to the Observatory for the Online Platform Economy", Analytical paper #7: Multi-homing: obstacles, opportunities, facilitating factors*, March 2021, page 8.

The 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 OESs and OVIs, for example, have to comply with certain constraints that may affect their use of the public cloud.

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

- cloud service customers who have chosen to use these services for some or all of their workloads, from an on-premise infrastructure.
- cloud-native companies, which 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 around these services. These companies therefore do not need to transform their IT systems in order to migrate to the cloud.

Cloud service customers also come in all sizes. Migration to the cloud involves all categories, whether large enterprises, mid-sized companies, SMEs, VSEs or public entities, although the criteria for the choosing a cloud service provider tend to vary according to the category of customer.

In France, this sector is expected to grow by around 14% a year, reaching 27 billion euros by 2025. However, the adoption of cloud services in France is lagging behind, with SMEs and VSEs 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 email (67%). However, storage and computing capacity services appear to be the most widely used, especially when compared with PaaS services.

Finally, even if companies want to implement multi-cloud, they typically only use one cloud service provider for a given workload, due to the necessary investments in time, money and technology as well as the complexity of such projects, for example to ensure the necessary compliance with regulatory standards.

C. THE DIFFERENT OPERATORS IN THE CLOUD VALUE CHAIN

77. The cloud value chain includes data centre operators at the upstream level (a), cloud service providers at the center (b) and integrators at the downstream level (c). Some players tend to position themselves across the entire value chain, while others focus on a limited segment. Several providers also offer marketplaces open to third parties (d).

a) Data centre operators

78. The provision of cloud services uses physical infrastructures hosted in data centres. These centres are secure physical spaces, powered by electricity and interconnected with telecoms networks. Building a data centre takes several years and major investments.

79. Companies such as Colt, Data4, Equinix, Global Switch and Telehouse specialise in building and operating these infrastructures. They offer space rental and a range of associated services (connection, security, air conditioning, etc.). Some operate on a leasing model, whereby their customers pay them a monthly rent in exchange for operating a "clean room". Others provide co-rental infrastructure for all types of customers, with contracts generally ranging from three to five years.

80. Space rental is offered to different types of customers, such as network operators, SaaS providers, companies from all sectors wanting to host IT infrastructures, and public cloud service providers. These providers can install their servers in data centres and then offer their services. Data centre operators are therefore upstream in the value chain, and not directly considered as cloud service providers.

81. Pricing for their services generally depends on the amount of space rented within the data centre (number of racks, square metres, any secure spaces, etc.), use of electricity, connectivity and the remuneration of employees present in the centre. The major data centre operators work on a large scale, owning data centres in several countries, that are operated in a standardised way (standard contract, similar services and processes) so that international customers wanting to expand into several countries can use the service in these countries, as close as possible to their businesses.

82. The investigation showed that some cloud service providers, such as Google Cloud and Scaleway, build their own data centres for all or part of their needs, thus moving up the value chain. For the time being, however, it appears that these cloud service providers are not in direct competition with the centre operators, insofar as their centres are dedicated to their exclusive use.

83. Given the specific nature of their activities, data centre operators are not included in the main scope of analysis in the rest of this opinion.

b) Cloud service providers

84. Cloud providers consist of all companies offering virtualised IT services that are adaptable to the user's needs.

85. These providers can therefore position themselves on one or more IaaS, PaaS or SaaS models, or even on one or more specific services. Some providers choose to offer extensive ranges of cloud products or services to cover the majority of customer needs. This can require control of the entire value chain, from the design of the servers to the design of the cloud platform solutions provided to their customers, as well as the construction and management of their data centres and the orchestration of their fibre network. Other providers, on the other hand, may concentrate on a particular part of the market, offering hosting and IaaS services only, or a specific PaaS or SaaS service to be marketed through different channels (software resellers, provider marketplaces, etc.).

86. Cloud service providers have different positioning, business models and stages of development which makes their description complex. The main categories likely to be proposed are set out below.

Providers already present in the digital sector

Hyperscalers

87. As mentioned above, the term *hyperscaler* is commonly used in the cloud industry to refer to major cloud service providers with very large and expanding capacities.

88. Of the cloud service providers, the three largest - AWS, Google Cloud and Microsoft - share several similar characteristics that tend to bring them closer together. All three belong to major digital companies that are among the world's largest market capitalisations. They already have a strong presence in digital services markets and have leveraged their considerable financial resources and internal needs to build up IT capacity worldwide and offer a large number of diverse cloud services, which have subsequently formed ecosystems[97] (see Part II.C).

89. Nevertheless, each of these companies has been able to build on its original market(s) to offer value-added services and solutions in the public cloud market. As a result, despite a number of shared characteristics, the way in which these companies entered the cloud sector and their business models differ in many respects.

90. For the sake of convenience, and given their leading position in the French market, the *Autorité* considers that these three main players can be referred to as hyperscalers in the remainder of this opinion. Other companies, such as Alibaba and Oracle Cloud, have entered the French market more recently, but share certain characteristics with these providers and could join this category in the future.

♦ *Amazon Web Services (AWS)*

91. As mentioned above (see paragraph 15), in 2006 Amazon decided to make its cloud infrastructure available to other developers and companies, who could then benefit from scalable and modular on-demand computing resources, accessible via the Internet and paid for on a pay-per-use basis.

92. Amazon was the first company to offer such a public cloud model worldwide. Today, AWS is still considered the market leader, with over 200 cloud services offered in most countries around the world. Its expertise has historically focused on the IaaS model, with flagship services for storage (Amazon "S3"[98]) and computing (Amazon EC2), as well as PaaS (notably with Amazon RDS[99], a relational database management tool, and AWS Lambda, the serverless reference service[100] according to AWS). Every year, the company launches dozens of new cloud services, including new functionalities based on artificial intelligence and machine learning technologies.

[97] Ecosystems have been defined as "*a number of firms – competitors and complementors – that work together to create a new market and produce goods and services of value to customers*" (Digital Economy: Joint report by the Autorité de la concurrence and the Competition and Markets Authority on the economics of open and closed systems, December 2014, link).

[98] Read more about Amazon "S3" in Part IV.

[99] Amazon Relational Database Service is a set of managed services that make it easy to configure, use and scale databases in the cloud (link).

[100] AWS and other providers offer technologies that enable code execution, data management and application integration, all without the need to manage servers.

93. AWS's customers include major digital services companies such as Airbnb, Netflix and Pinterest, which have been able to grow very rapidly, not least thanks to the possibilities offered by the public cloud. In France, startups such as Doctolib, OpenClassrooms and Reezocar, as well as major corporations such as SNCF and Société Générale, have also used AWS services.

94. By 2022, AWS, with a turnover of $80 billion, accounted for around 16% of Amazon's worldwide turnover, up by more than $17.8 billion year-on-year (+29%)[101]. AWS revenues have been growing strongly since the launch of the services and are also generating substantial profitability. AWS is thus Amazon's most profitable entity, accounting for 74% of its operating income in 2021[102].

♦ *Google Cloud*

95. Alphabet Inc. (Alphabet) is an American group of companies, the largest of which, in terms of sales and employees, is currently Google LLC (Google). Google operates an online search engine and has been offering other services to companies, including cloud services, since 2011. These cloud services activities are grouped together in its Google Cloud branch, created in 2018, and correspond to two main service offerings: Google Cloud Platform (hereinafter "Google Cloud") and Google Workspace.

96. Google Cloud is a corporate cloud offering that includes over 100 IaaS and PaaS products running on Google's infrastructure. It is perceived as the third-largest player in the public cloud and is particularly attractive for the provision of data analysis services, artificial intelligence and machine learning tools. Its customers come in all shapes and sizes and operate in a wide range of sectors.

97. Google Workspace is a set of productivity applications for companies and governments (SaaS), including communication, collaboration and administration services[103].

98. The Google Cloud entity has achieved $26 billion in turnover by 2022, up 37% compared to 2021[104]. For the first time since its creation, Google Cloud posted an operating profit ($191 million) in the first quarter of 2023[105].

♦ *Microsoft*

99. Microsoft Corp. (Microsoft) is an American technology company offering a wide range of technology products, including cloud services. Microsoft is a long-standing provider of computer operating systems (Windows) and office software (Office). The company has been active in the public cloud since 2010, with Azure and its most popular software now offered as SaaS. Microsoft currently offers over 130 cloud services.

100. Microsoft's "Intelligent Cloud" segment covers activities related to the IaaS and PaaS models (public, private and hybrid) with Microsoft Azure, as well as Windows Server, Microsoft

[101] Amazon, Annual Report 2022, page 23 (link).

[102] Amazon, Annual Report 2021 (link).

[103] See, for example, the *"Google Workspace for Government"* offer on the Google website (link).

[104] Alphabet, Annual Report 2022, page 32 (link).

[105] Alphabet, Q1 2023 financial results, page 39: "*Google Cloud operating income of $191 million for the three months ended March 31, 2023 compared to an operating loss of $706 million for the three months ended March 31, 2022 represents an increase of $897 million*" (link).

SQL Server, Visual Studio and corporate services. This segment recorded a turnover of $75.2 billion in 2022, up 25% compared to 2021. Its operating income also increased by 25% between 2021 and 2022, to represent 39% of the total income[106].

101. Microsoft Azure offers data processing and storage, networking, runtime operating systems and middleware.[107] These services are distributed to customers of all sizes and in all sectors but are mainly aimed at developers, IT professionals and companies. Azure's revenues are set to increase by 50% between 2020 and 2021[108]. Microsoft Azure is generally considered to be the second-largest player in the IaaS and PaaS market, and the best solution for running Microsoft software.

102. SaaS services account for the largest percentage of Microsoft's cloud services turnover, driven mainly by Microsoft 365 and Dynamics 365. Microsoft 365 is a software suite distributed as a SaaS and offering work environments and interfaces for companies and public administrations, with basic functionalities for collaboration, communication and productivity, as well as options available on demand. Dynamics 365 is a modular SaaS offering, under which Microsoft sells its intelligent business applications, resource planning systems and customer relationship management solutions. These offers are aimed at companies of all sizes, in all sectors, and at public sector operators.

Other companies from the software and business information systems sector

103. Other providers in different markets who have expanded into cloud services include companies from the intermediation services sector, such as Alibaba, and from the software and corporate information systems sector, such as IBM and Oracle. These companies share some characteristics similar to hyperscalers, but are currently undergoing less rapid development in the French market.

♦ *Alibaba Cloud*

104. Alibaba Cloud is an entity founded in 2009 by Alibaba Group, a Chinese company offering an e-commerce platform. Alibaba Cloud, which has been in France since 2016, currently offers services in over 200 countries and distributes over 200 cloud services (IaaS, PaaS and SaaS). Its activity is still emerging in France and the European Economic Area. The company positions itself primarily as a provider able to support European companies wanting to access and connect to the Chinese market. Currently, 60 to 80% of its turnover in France comes from IaaS services.

♦ *IBM*

105. IBM is an American company specialising in information technology. It develops, produces and markets business software and IT systems (servers, storage systems, etc.) as well as IT implementation services (consulting, infrastructure, etc.).

106. In the cloud sector, it offers services to companies worldwide. IBM has expanded in this segment with the 2019 acquisition of Red Hat, which specialises in open-source software and support services. Through these different entities, the company offers an IaaS offering,

[106] Microsoft, Annual Report 2022 (link).

[107] According to Microsoft, middleware refers to a broad category of software products located between the operating system and the application software, providing the necessary infrastructure for running or accessing applications. Printer drivers, for example, are middleware.

[108] Microsoft, Annual Report 2021 (link).

a multi-cloud PaaS offering based on Kubernetes (Open Shift), PaaS offerings for databases and developer tools, and over 150 SaaS solutions for companies. These services are offered in France and Europe, via ten data centres located in Europe and owned by third parties.

♦ *Oracle*

107. Oracle offers a range of cloud services at every level of the value chain. The company expanded in this sector, first with software solutions offered as a SaaS model from 2005 and then, since 2014, with IaaS and PaaS services. The development of its cloud activities has been facilitated by a number of company acquisitions and by its already well-established presence with a large number of companies in the form of on-premise solutions distributed via perpetual licences. In this respect, Oracle's business model is very similar to that of Microsoft.

108. Oracle's flagship cloud products are (i) the Business Suite (SaaS), a suite of company software customised for each business sector, (ii) Oracle Database (PaaS), a managed database[109] and (iii) the Oracle Cloud Infrastructure (OCI) in IaaS. At the end of 2022, Oracle Cloud had more than 40 cloud regions worldwide, including two data centres in France, enabling it to offer services in the majority of countries.

109. As its technologies have historically been used by public administrations and governments, Oracle is keen to position itself as a trusted partner and is developing offers with a strong emphasis on security. Oracle has also entered into a strategic partnership with Microsoft, enabling customers to connect their Oracle Cloud Infrastructure and Microsoft Azure resources *via* a dedicated private connection, and to deploy Oracle software in Microsoft clouds with Oracle certification and support[110].

Electronic communications operators

110. Several electronic communications operators, such as Orange and Bouygues Telecom, also distribute cloud services. They enjoy long-standing relationships with companies for the provision of communications and Internet access services.

111. In addition to their own cloud infrastructure offerings, some players, such as Orange, are positioning themselves to support businesses in moving and maintaining their IT activities in the cloud, and have forged partnerships with infrastructure providers. Their positioning is more akin to that of an integrator (see *c below*).

Pure player providers

112. Other providers can be described as "pure players", insofar as their activities mainly concern the cloud, and they have little or no presence in other markets. Some offer a wide range of complete IaaS and PaaS services available to customers. Others, on the other hand, specialise in certain services or categories of cloud services.

Generalist providers

113. Among the pure players, some providers offer a range of cloud services to cover the majority of business needs, particularly in IaaS and PaaS. Their range of services is currently less

[109] Oracle defines a managed database as "*a database with storage, data, and compute services that is managed and maintained by a third-party provider instead of by an organization's IT staff*" (link).

[110] See the Oracle Cloud website (link).

extensive than those of hyperscalers. Leading French providers such as OVHcloud, Scaleway and 3DS Outscale fall into this category.

♦ *OVHcloud*

114. OVHcloud is a French cloud services provider offering public and private cloud solutions, shared hosting and dedicated servers in 140 countries. Founded in 1999, this company specialised in the cloud web (domain name allocation, web hosting and website services, etc.), before expanding into the private cloud and more recently the public cloud. This last segment still accounts for a small percentage of its turnover but is growing fast. OVH offers integrated IaaS and PaaS solutions and has over 30 of its own data centres (in France, Europe, North America, Singapore and Australia) as well as its own fibre optic network.

♦ *Scaleway*

115. Scaleway is a French company and a subsidiary of the Iliad Group, specialising in public cloud services. Founded in 1999, this company initially offered hosting services, then gradually expanded into the public cloud in the 2010s. Scaleway offers an integrated model of IaaS and PaaS services, with the latter being a key strategic development area.

♦ *3DS Outscale*

116. 3DS Outscale is a French company founded in 2010 and part of the Dassault Systèmes Group. It mainly distributes highly secure IaaS solutions. The main customers interested in these offers are French players with major security concerns, such as public administrations, OVIs and OESs.

Specialised providers

117. There are also many providers who specialise in PaaS and SaaS services and generally run their services on the infrastructure of IaaS solution/service providers. For example, Platform.sh offers a PaaS hosting platform *via* its partnerships with Amazon, Google, Microsoft, Orange and OVHcloud. Jamespot and Whaller offer SaaS solutions for corporate social networking and collaborative platforms, hosted on the IaaS infrastructures of French providers. These players therefore have the particularity of being considered both cloud service providers and customers of other providers.

Providers aiming to offer "trusted cloud" services

118. In response to regulatory changes and the launch of the "trusted cloud" doctrine (see paragraphs 47 et seq. above), cloud service providers are positioning themselves with specific offerings. For some, this may mean extending their range of services to include SecNumCloud-certified offerings. For others, it requires the creation of new partnerships dedicated to the marketing of these offerings under development.

SecNumCloud providers

119. By September 2022[111], five cloud service providers - Cloud Temple, Oodrive, OVHcloud, Worldline and 3DS Outscale - had SecNumCloud-certified offerings (seven certified

[111] Press release, "Bruno Le Maire and Jean-Noël Barrot reaffirm the national cloud strategy and announce new measures to support the sector", 12 September 2022 (link).

offerings in total). These offers have been made available in particular to public sector customers holding sensitive data.

Alliances in the making

120. Several operators have announced alliances or partnerships aimed at creating "trusted cloud" offerings. Of these, several American hyperscalers have announced that they are involved in the development of offers that can be labelled "trusted cloud" thanks to their association with French players. In May 2021, integrator Capgemini and electronic communications operator Orange announced their intention to create Bleu, in partnership with Microsoft, which will provide its Azure services but remain outside Bleu's governance and not hold any shares in the new company[112]. Similarly, in June 2022, Google Cloud and Thalès[113] presented a strategic partnership to create the company S3NS, also aimed at marketing "trusted cloud" offerings. In addition, four French players - Docaposte, Dassault Systèmes, Bouygues Telecom and *Banque des Territoires* - announced in October 2022 that they were joining forces to offer a "trusted cloud" offer - NUMSPOT - available in 2023[114]. According to press reports, AWS and the integrator Atos are also preparing a similar offer[115]. None of the offerings resulting from these alliances is currently being marketed or has been certified as SecNumCloud.

c) Integrators

121. Integrators support cloud services customers in managing their migration to the cloud and in upgrading and maintaining their applications in the cloud in working order. These players can be (i) digital services companies (hereinafter "DSCs"), such as Accenture, Atos, Capgemini, or Orange (via its Orange Business Services brand), (ii) small, specific players, such as Padok, who support companies in the transition from on-premise infrastructure to IaaS, or (iii) business units of companies that are otherwise cloud service providers, such as IBM (*via* IBM Consulting).

122. These companies play a key role in helping users of cloud services to choose the right solutions and in implementing and upgrading their information systems. Thanks to their partnerships with numerous cloud service providers (with hyperscalers at the forefront), they offer their customers customised packages, combining the provision of several cloud services with additional building blocks to ensure the smooth running of the entire architecture. They are also positioned as resellers of specific cloud services, and for the most part are able to provide a set of services tailored to all cloud environments. These companies have human resources with cross-disciplinary skills.

123. Of the customers surveyed by the *Autorité*, 50% said they had used the services of at least one integrator when migrating to the cloud. The integration market is booming, with estimated annual growth of 13% in France between 2021 and 2025.

[112] Press release, "Capgemini and Orange announce plans to create "Bleu", a company that will provide a "trusted cloud" in France", 27 May 2021 (link).

[113] Thales website, "Thales introduces S3NS in partnership with Google Cloud and unveils its offering in a first step towards the French trusted cloud label", 30 June 2022 (link).

[114] Direction Générale des Entreprises portal, "NUMSPOT: a partnership for a new trusted cloud service", 26 October 2022 (link).

[115] L'Usine digitale, Amazon and Atos take their turn in the "trusted cloud", 17 October 2022 (link).

d) Cloud marketplaces

124. Independent software providers without their own infrastructure can (i) sell their services directly to users, (ii) use resellers (often integrators) who bundle their solutions with other services, and/or (iii) be reference listed on a cloud service provider's marketplace, in which case the service sold will run on the provider's infrastructure.

125. Cloud marketplaces are platforms managed by a cloud service provider on which their customers can access solutions from other cloud service providers or independent software publishers. For example, Alibaba Cloud, AWS, Google Cloud, IBM, Microsoft Azure, Oracle and OVHcloud all have their own marketplace. Some of these marketplaces also market their own services (mainly SaaS). While some providers with their own marketplace also sell their services on other marketplaces, this is generally not the case for hyperscalers. Third-party sellers can generally offer services similar to those of marketplace operators. Marketplaces range in size from a few dozen to over 10,000 services, with AWS being the most developed.

126. To become a seller on a marketplace, it is essential to accept the platform's terms and conditions, which are available on the provider's website. The use of a marketplace by third-party publishers gives them a channel for marketing to the users of a cloud service provider that includes a set of services such as transaction provisioning and revenue remittance. In return, marketplaces generally charge a commission on sales, at least to cover their operating costs.

127. The information collected by the investigation services indicates that the prices charged on the providers' marketplaces have also evolved over the last few years, with some players reducing prices and with a wide variety of commission rates depending on the solutions proposed by the sellers. The rates currently being applied seem to be fairly aligned between marketplaces, at around [0-5] %, with the exception of AWS, which varies between [0-30] %.

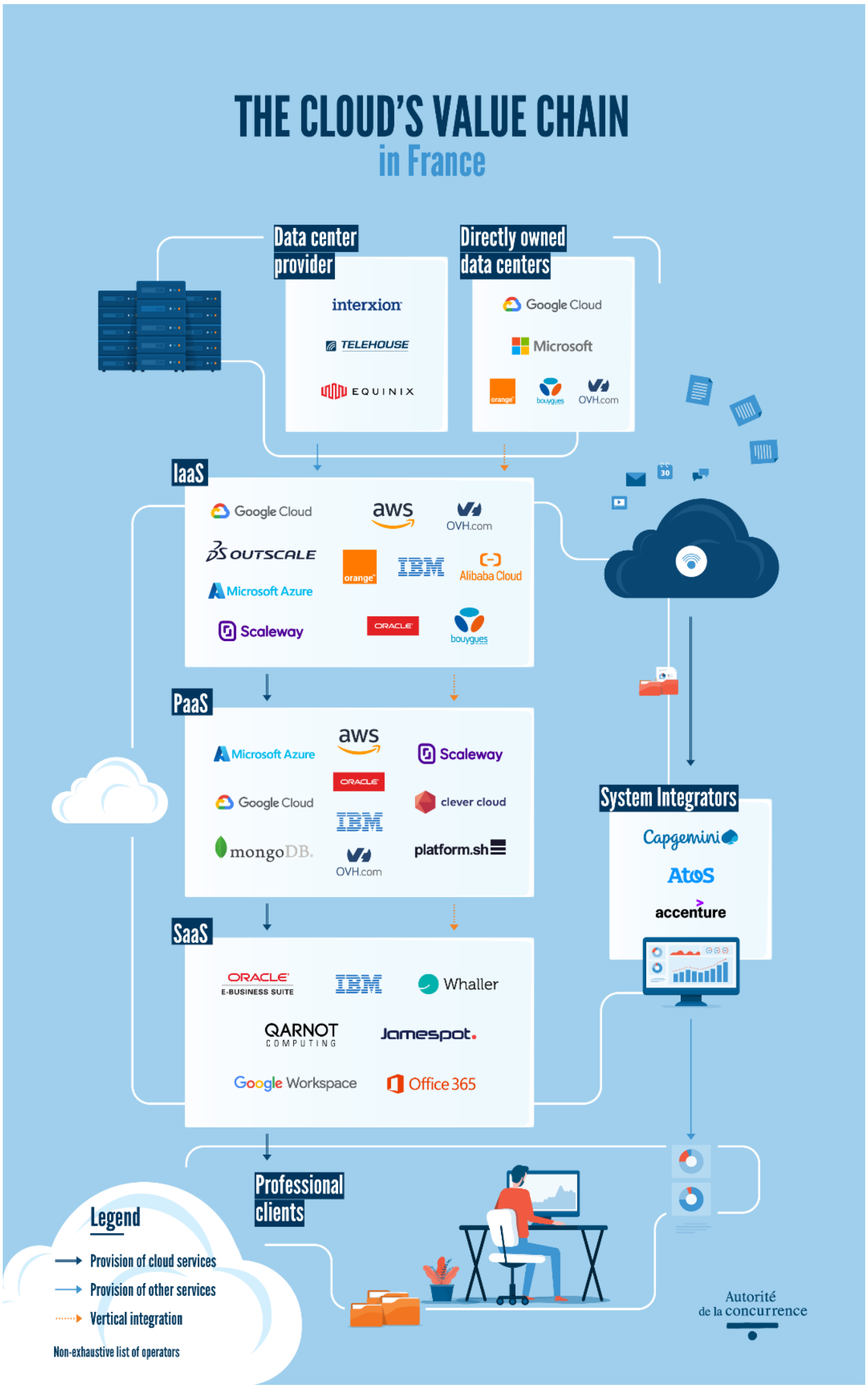
128. Customer feedback has shown that, for the vast majority, the level of commission charged by marketplaces, and its evolution, is not a matter of particular concern. One customer, however, considered it legitimate to fear an increase in commissions as hosting providers become essential while pointing out that in the short term competitive pressure remains sufficient.

129. At present, marketplace services make up only a tiny proportion of cloud service providers' business and revenues. By way of illustration, revenues from solution downloads represented just 0.01% of the total cloud revenues of one hyperscaler in France in 2020[116]. During the investigation, cloud service providers told the *Autorité* that they expect this percentage to rise slightly over the next few years, although they consider that it will remain minimal.

130. Figure 13 below summarises the different players in the cloud value chain in France.

[116] Autorité's calculation based on data supplied by the hyperscaler concerned.

Figure 13 - The cloud value chain in France



Source: Autorité de la concurrence

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 hyperscalers, companies from the software and business information systems sector, or electronic communications operators;
- pure players, insofar as their activities mainly concern the cloud, and they have little to no presence in other markets.
- providers aiming to offer certified "trusted cloud" 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. While some providers with their own marketplace also sell their services on other marketplaces, this does not seem to be the case for AWS, Google Cloud and Microsoft. Third-party sellers can generally offer services similar services to those of marketplace operators.

D. THE RELATIONSHIP BETWEEN CLOUD SERVICE PROVIDERS AND THEIR CUSTOMERS

1. CONTRACTS

131. Standard contracts apply to the majority of customers, with only a few large-scale consumers of cloud services seeming to succeed - on an exceptional basis - in obtaining more favourable financial terms. On the one hand, standard contracts entered into directly on the supplier's website, involve acceptance of the general terms and conditions of service, without negotiation. They are generally open-ended and can be terminated at any time. On the other hand, more personalised contracts apply to certain key account customers. These contracts include certain negotiated clauses and possibly a commercial discount in return for the use of a certain volume or value of services. They are generally fixed-term contracts, varying from one to three years.

132. Several providers have indicated that they offer a discount to customers purchasing larger volumes of services. For example, Google offers "Committed Use Discounts" on certain products[117]. Microsoft, offers “Enterprise Agreements” to its largest customers for all the Microsoft products and services they purchase[118]. The "Microsoft Open Value" programme also offers smaller customers the opportunity to obtain fixed prices for the duration of the

[117] Committed Use Discounts, can be consulted online (link).

[118] Entreprise Agreement, presented online (link).

agreement in return for a commitment to order enough licences to cover their entire organisation[119].

133. The contracting process and customers' ability to negotiate in a cloud deployment mode differ from the on-premise model, in particular due to a change in the relationship between customer and provider. Customers move from purchasing fixed resources (non-flexible and non-expandable) at a predictable, negotiated cost, to leasing modular resources (flexible and expandable) but at a price that is difficult to estimate (see Part IV below).

134. Cloud service providers also use resellers to reach a wider audience. In particular, IaaS service providers use this indirect sales channel to integrate their services into more comprehensive offerings that better meet customer needs. In this case, the provider and reseller enter into either framework contracts generally lasting between one and three years, or open-ended contracts. However, apart from public procurement contracts, for which invitations to tender through UGAP are mandatory, invitations to tender are a very marginally used sales channel.

2. USAGE-BASED PRICING

135. Usage-based pricing is generally applied per unit, for example on the basis of seconds of computing power or per gigabyte stored. The customer thus receives a regular invoice corresponding to their actual use of the services. The prices may depend on a range of parameters, such as geographical regions or subscriptions to premium options. Some providers also charge their customers for outgoing or inter-regional data transfers (see d. below Egress fees).

136. Depending on the provider, prices of service may vary according to the nature of the service, underlying capital and operating costs, customer demand and the price of competing offers. They generally give 30 days' notice of price increases.

137. While providers commonly display all their prices in detail and publicly on their websites, on the basis of actual use of services ("pay-as-you-go" model), the investigation showed that most customers face a lack of transparency with respect to prices and find it difficult to anticipate their cloud service budgets. Firstly, this may be linked to difficulties in accurately assessing their needs, particularly when they first start using the services. The first purchase is made with uncertainty regarding the costs of subsequent purchases, such as the use of complementary products or services, or even the possibility of changing provider easily.

138. Furthermore, the information collected in the course of the investigation shows that the clarity of the prices charged by some cloud service providers can be relatively limited for many customers. Several players pointed out the complexity of certain catalogues, invoices and egress fee calculations, further aggravated by the frequency of changes. To meet this challenge, some providers, such as AWS[120], Google Cloud[121] and Microsoft[122], offer a cost simulator, which can help improve clarity. However, according to a study by *KPMG* published in April 2021, *"the pricing models of European providers appear to be more*

[119] Microsoft Open Value programme, presented online (link).

[120] AWS Pricing Calculator, available online (link).

[121] Google Cloud Pricing Calculator, available online (link).

[122] Azure Pricing Calculator, available online (link).

transparent than those of hyperscalers, who currently dominate the market with often aggressive and unconventional customer acquisition practices (e.g. tied selling of SaaS and IaaS services), as well as complex exit conditions, which make it difficult for cloud users to leave a provider or move from one provider to another"[123].

139. Finally, as the prices are generally not fixed in the contract, providers can therefore unilaterally revise the pricing schedule or schemes on a regular basis. The investigation showed that several customers have faced pricing changes and costs that could not have been anticipated. Several practices from providers (see Part IV) relating to service pricing or egress fees are described in greater detail below, in view of the competitive risks they are likely to raise.

3. CLOUD CREDITS

140. Cloud credits are trial offers in the form of service allowances offered by a provider and granting free access to a customer within a defined period. In practice, and as the *Autorité* recalled in its Opinion 23-A-05[124], unlike a free trial, it is a sum to be spent in the form of an invoice credit granted before use.

141. Credit programmes are representative of a "freemium" business strategy, offering access to a product or service free of charge in order to attract as many users as possible, and then offering a paid version. The freemium model exists in many digital sectors, including software sales, video games, on-demand video and music platforms and social networks. This model is defined by a free offer with limited functionalities, ease of use or time. In the case of the cloud, the user is restricted by the credit mechanism, which limits storage capacity, the number of licences, the variety of products or services and the time of use. Free, limited access to certain functionalities very often replaces or supplements the credit offer: some providers only offer free trials and others mainly offer programmes in the form of credits, often combining the two on different products and services.

142. Cloud credit programmes are not always limited to a particular service or product and may apply to the entire range of services or products offered by a provider. The responses to the customer questionnaires collected during the investigation show that credit offers, and more generally free support, are more common for the IaaS layer (56.5% of respondents) than for the PaaS (39.1% of respondents) and SaaS (34.8% of respondents) layers[125]. Customers can take advantage of several programmes at once or one after the other, subject to the specific conditions governing the programmes (e.g. customer seniority or stage of financial development of the company).

[123] KPMG, "The European cloud: major challenges for Europe and five scenarios with major impacts by 2027-2030", April 2021, page 7. Report drafted for Talan SAS, InfraNum, OVHcloud and Linkt.

[124] https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/informatique-en-nuage-cloud-lautorite-de-la-concurrence-emet-un-avis-sur.

[125] Source: AMF calculations based on the online customer questionnaire, in particular the number of customers responding to the questionnaire and declaring that they receive free credits or support on the identified layer, in relation to the number of customers responding to the questionnaire.

a) Programme types

143. There are many cloud credit strategies that vary between providers. There are two main categories of cloud credit offers, depending on whether they are based on testing and discovering a provider's products and services (free trial-type programmes) or targeted at specific players due to particular attributes (support programmes).

144. One of the primary aims of cloud credits is to encourage new customers to adopt cloud services, enabling them to take the risk of experimenting with new technologies and testing new services without bearing the associated cost. A number of cloud credit programmes are available for new customers or for existing customers wanting to test new functionalities. The aim is to enable customers to assess product performance in real-life situations, and then, after a trial period, to propose that they adopt the tested solution.

145. The *Autorité* found that most cloud service providers offering cloud credits offer the first type of programme. On the hyperscaler side, the AWS Proof of Concept programme offers $1,000[126] in promotional credits with no apparent time limit, which is relatively more than Google Cloud's $300[127] over 90 days and Microsoft Azure's $200[128] over 30 days. Like Google Cloud, Oracle has a $300 offer, but for a more limited 30-day period[129]. French cloud provider OVHcloud and IBM are offering almost the same amount as Microsoft - 200 euros[130] in coupons or 200 dollars[131] in credits over 30 days. Scaleway's offer is half that amount (100 euros of credits over 30 days[132]). Smaller providers also offer credits for trial purposes, but at much lower prices; Clever Cloud, for example, offers 20 euros worth of credits[133], while Qarnot Computing offers 15 euros[134]. Lastly, other providers, such as Orange[135] or Platform.sh[136], offer free support or access to their services for test purposes, for varying lengths of time, without this taking the form of credits (pure freemium).

146. As mentioned in Opinion 23-A-05, 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, for a limited period of time, and can be frequent or recurring, with a cloud service provider potentially offering new cloud credits each time it offers a new service.

147. Other credit programmes are aimed exclusively at certain target groups, in particular those with a high innovation potential, such as startups, developers, researchers and students. These programmes could be described as support programmes.

[126] AWS Proof of Concept programme.

[127] Free Google Cloud programme.

[128] Free Azure account.

[129] Oracle Cloud Free Tier.

[130] Public Cloud OVH Free trial.

[131] IBM Cloud free Tier.

[132] Promotional code "TRYSCALEWAY" for new customers.

[133] clever-cloud.com.

[134] Qarnot, free trial: €15 free.

[135] Orange Flexible Engine.

[136] Platform.sh free trial.

148. Providers are competing fiercely for promising young companies such as startups. While startups are considered by a major cloud service provider to be companies that "*experiment a lot but often fail*", they have substantial growth potential that needs to be conquered quickly. According to one cloud service provider, the aim in targeting these startups is to ensure that "*future discoveries and solutions are directly built and integrated with reference to* [*their*] *ecosystem*". This is particularly crucial as many of the startups covered by the credit programmes are cloud native.

149. The credits would enable them to test providers' products and services, be supported in their research and development process, and alleviate their infrastructure costs at an early stage of the company when most have little or no revenue. The objective is to support them and give them the benefit of computing capacities and a range of cutting-edge tools without forcing them to draw on their capital but at the same time building loyalty. Credit programmes for startups can also be coupled with mentoring and personalised coaching.

150. For startups, Google Cloud offers up to $200,000 in credits over two years[137], Microsoft Azure up to $150,000[138] and AWS up to $100,000[139]. The offers of Clever Cloud and OVH are similar to those of AWS (100,000 euros in progressive rebates[140] or technology credits[141]). Two other French providers have offers, but for lesser amounts: up to 36,000 euros[142] of credit over one year from Scaleway, and an endowment of 20,000 euros[143] over three months from 3DS Outscale. This is comparable to IBM's offer of up to $18,000[144] in credits for six months.

151. On the university research side, the amounts and programmes are varied, but offers seem to be concentrated among hyperscalers. Google Cloud offers up to $5,000[145] in credits to researchers for their projects (obtaining computing power, for example), whereas there is no limit to the amount of promotional credits available under the AWS programme[146]. Microsoft Azure offers a way for researchers to apply for grants of up to [$25,000 - $90,000] when their work involves artificial intelligence.

152. Cloud credit programmes are also aimed at students or recent graduates, who are more aware of digital technologies and also have the potential to use products and services for relatively longer. Offers to students range from $100[147] and $200[148] over a year at Microsoft Azure and Google Cloud respectively, to $300[149] at Oracle, while those for graduate students and/or

[137] Google Cloud for Startups programme.

[138] Microsoft for Startups programme.

[139] AWS Activate programme.

[140] Early Stage by Clever Cloud.

[141] OVHcloud Startup Programme.

[142] Startup Program Growth Stage Scaleway.

[143] Outscale for Entrepreneurs.

[144] Startup with IBM Startup with IBM.

[145] Google Cloud for researchers Google Cloud for researchers.

[146] AWS Cloud Credit for Research.

[147] Microsoft Azure for Programme for students.

[148] Google Cloud Programme for students.

[149] Oracle Academy Cloud Programme.

PhDs, at AWS for example, can be up to $5,000[150]. In the field of education and research, IBM[151], Oracle[152], Scaleway[153] and 3DS Outscale[154] take a parallel approach to cloud credits, offering educational initiatives and resources for students and recent graduates, in the form of courses, conferences, workshops, hackathons[155] or graduate programmes. Last but not least, Microsoft Azure offers a monthly credit package dedicated to developers[156], in particular those who subscribe to Microsoft Visual Studio, a range of development software from Microsoft.

153. To a lesser extent, specific programmes are aimed at non-profit organisations to enable them to implement cloud-based solutions. AWS and Microsoft Azure offer them $1,000[157] and $3,500[158] in credits respectively. Providers also have special programmes for their partner companies with which they share common customers, and these companies can unlock various financial benefits. For example, Microsoft Azure's offer reached around 4,000 companies in 2021 and ranged from $100 per month to $13,000 per year[159].

154. As pointed out in the aforementioned Opinion 23-A-05, cloud credits offered in the form of support programmes are mainly offered by the largest cloud service providers to users with high innovation potential, such as startups, cover much higher amounts than cloud credits offered in the form of tests (hundreds of thousands of euros, for example), and can last for several years.

155. In addition to credit programmes, which represent predefined, structured offers, cloud credits can also be granted on the basis of direct discussions between customers and providers. According to one hyperscaler, credits can be offered to customers on a case-by-case basis depending on a range of parameters, based on usage scenarios, for example. Another hyperscaler confirmed that the aim of bilateral commercial discussions remains the same as for programmes in general: "*to use and test the performance of services and compare existing services on the market*".

b) Using cloud credits in practice

156. The average validity period of cloud credit discounts and the amount provided depend on the programme and the provider. Validity seems to vary from one month to several years. One hyperscaler reported that the average duration of the credits it paid to accounts opened in 2021 was around seven months, compared with one year in 2019 and 4.5 months in 2020.

[150] AWS Cloud Credit Programme for Research.

[151] IBM Cloud for Education.

[152] Oracle Academy Cloud.

[153] Scaleway Academia Program.

[154] Education Outscale Programme.

[155] A hackathon or programming marathon is an event during which groups of volunteer developers come together for a given period of time to work collaboratively on computer programming projects.

[156] Azure Programs for Developers.

[157] AWS Nonprofit Credit Program.

[158] Azure resources for nonprofit.

[159] Azure program for Partners.

157. In terms of volumes granted, in 2021, a hyperscaler would have around [5,000 - 10,000] credit accounts for all its customers. This figure is rising steadily, so that for this provider, the number of accounts[160] receiving credits more than doubled between 2017 and 2021, and the value of the credits more than quadrupled between 2020 and 2021[161]. According to the hyperscaler, however, the value of the cloud credits granted to customers should be considered with caution, as it does not reflect the actual cost of provision for the hyperscaler, which is in fact much lower.

158. It should also be noted that the credit amounts offered in the programmes must be distinguished from the amounts actually used by customers. On the one hand, some programmes have eligibility criteria that restrict access, so not all customers can receive the maximum amount advertised. On the other hand, various providers agree that the allocated credits are never used in full.

159. One hyperscaler pointed out that the programmes may initially appear substantial, but in reality they are rarely used and/or selective: only [30-40] % of the members of its startup programme have actually used the cloud product/service offered to them in the credit package, and only [5-10] % have reached a level of development that enables them to qualify for the maximum credit amount. The overall impact of its programme targeting 2,000 startups is relatively low, since between 2018 and 2021, customers in France only used on average around [20-30] % of the credits offered. In this respect, one customer confirmed that it "*receives cloud credits as a customer, but does not always use them*". For another hyperscaler, in 2021, the actual credit utilisation rate by its [1,000-5,000] startups was even lower, averaging [1,000-5,000] dollars out of the [50,000-150,000] dollars on offer.

160. Although utilisation rates may be low for some hyperscalers, the credit volumes granted remain disparate between providers. It can be seen from the previous point that the value of the startup-targeted programme of the last hyperscaler quoted was in the order of [1-50] million dollars, which should be set against the statements of another hyperscaler, according to which the total value of cloud credits usage for its startup programme in France in 2021 was just over [200,000 - 500,000] dollars in total. This lower value can be explained by a smaller number of participating companies, around [100-500], i.e. [10-50] times less. A third hyperscaler announced a nominal value of [10-100] million euros in credits granted for the same year, but for all its programmes in France. By way of further comparison, one French provider indicated that the total amount of credit it had distributed, mainly to startups, was in the region of [1-10] million euros in 2021.

161. These cloud credit practices are analysed in greater detail in Part IV, with regard to their potential effects on competition.

4. EGRESS FEES

162. As the *Autorité* recalled in its Opinion of 20 April 2023[162] regarding the French draft law to secure and regulate the digital environment,, some cloud service providers, particularly the

[160] A given customer may hold several accounts.

[161] However, this increase is due to one particular event, namely the worldwide launch in 2020 of a credit promotion tool that raised awareness of cloud credits and increased their use.

[162] https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/informatique-en-nuage-cloud-lautorite-de-la-concurrence-emet-un-avis-sur.

hyperscalers, are implementing a cloud service delivery model based primarily on billing customers according to their use of outgoing bandwidth ("egress only pricing model")[163], whether it involves data transfers to another provider (in the case of a multi-cloud strategy or migration) or to the company's on-premise infrastructures (in the case of a hybrid cloud strategy). These pricing structures involve a cloud service provider charging egress fees for the transfer of data outside of its cloud infrastructure.

163. Egress fees may vary according to the geographical region of origin and arrival of the data, and depending in particular on the provider's network coverage and resources. Transfer charges may also apply to data flows over the bandwidth between two data centres that belong to the same *cloud* service provider but are relatively far apart geographically.

164. Finally, data transfers to the provider's cloud environment (ingress traffic) are generally free and unlimited (ingress free).

165. The pricing of egress fees is analysed in greater detail in Part IV, to assess any competitive issues linked to this practice.

5. PRICING CHANGES

166. Given the many changes in cloud service providers' pricing schedules over the last few years, it is difficult to accurately track the evolution of the prices charged by different cloud service providers.

167. According to the main providers, prices for each cloud service are trending downwards, due in particular to lower technological and operating costs (reduced computing costs, more efficient hardware and infrastructure, optimisation, etc.). One hyperscaler pointed out that "*the main pricing trend* [...] *is the continued reduction in prices for computing costs. Cloud service providers are constantly updating their data centre hardware to make it faster and more efficient. As new hardware is introduced, computing speeds increase and relative costs decrease*." This trend enables it to pass on "*these savings to end customers in the form of cheaper, faster virtual machines*". Several reductions have been recorded in recent years. According to a 2018 study by TSO Logic, AWS has cut prices 67 times since its launch in 2006, and customer workloads cost 73% less in 2017 than in 2014[164].

[163] The bandwidth flow refers here to the data traffic circulating on the wired, generally fibre, networks used by cloud service providers to connect their various servers and data centres around the world and to download and upload all their customers' data.

Network bandwidth is the data transfer capacity of a network, i.e. the volume of data that can be transported from point A to point B in a given time interval. On modern networks, it is generally expressed in millions of bits per second (megabits per second, or Mbit/s) or in billions of bits per second (gigabits per second, or Gbit/s).

The bandwidth costs incurred by a cloud service provider depend on the level of investment it has made in developing its own network. These investments may involve the company's own development of the entire wired network and other network equipment required for data transport, but a provider may also decide not to use a network of its own, and instead pay access fees to third-party networks, in particular those of national telecoms operators or other third-party cloud service providers with a local presence. Finally, a provider can position itself at an intermediate level of investment and adopt a hybrid strategy. In any case, a cloud service provider must pay access fees when customer data transits through third-party networks.

[164] Blog post published by the AWS editorial team, "New Research From TSO Logic Shows AWS Costs Get Lower Every Year", dated 24 September 2018 (link).

168. From the customer's point of view, prices for cloud services, especially traditional services such as storage, have not changed significantly in recent years. However, with the rise in cloud usage and the use of new services, some customers are reporting that their budgets are rising steadily. An article published by consultancy firm Gartner predicted in 2021 that by 2024, 60% of IT infrastructure managers would face cost overruns related to the public cloud, with negative impacts on their budgets for on-premise solutions[165]. To maximise the usefulness of their cloud spending, business customers are increasingly having to introduce in-house management practices ("FinOps"[166] approach) to optimise their usage and mobilise a large number of organisational functions. Several providers also offer their own consulting services to help customers improve their usage. One hyperscaler, for example, has set up a large specialist unit, with around [50 - 2,000] staff in France, whose role is to help customers limit cloud usage, optimise their costs and plan them better.

169. Furthermore, several corporate customers are anticipating rate increases in the short to medium term. In the short term, the risks seem to be mainly economic, linked to the energy crisis, shortages of certain components and the resulting rise in provider costs. Several providers have already announced price increases, such as Google Cloud in March 2022[167], OVHcloud in August 2022[168] and Scaleway in October 2022[169]. Faced with a slowdown in growth, several major providers operating in different digital markets could also raise their prices[170].

170. According to some key account customers, there is also a risk that prices will rise further once the market is more mature and customers are locked in. In its "*Magic Quadrant 2021*" report on public cloud infrastructure offerings, Gartner stated that customers had been pressured by AWS sales departments during contract renewals to increase annual spending commitments by 20%[171].

[165] Gartner article, "*6 Ways Cloud Migration Costs Go Off the Rails*", 7 July 2021 (link).

[166] Financial Operations - Monitoring and optimising cloud computing costs.

[167] Google Cloud website, "*Unlock more choice with updates to Google Cloud's infrastructure capabilities and pricing*", 14 March 2022 (link).

[168] In August 2022, OVHcloud announced a price increase of around 10% for its public cloud services from 1 November 2022, due to rising energy costs (link).

[169] Upcoming price changes, Effective on December 1st, 2022, published on 28 October 2022 (link).

[170] Les Echos, "*Faced with slowing growth, the Gafams seek to fight back*", 26 October 2022 (link).

[171] LeMagIT, "*Cloud: Gartner takes a hard line on AWS, Azure and GCP*", published on 5 August 2021 (link).

The relationship between cloud service providers and their customers

Two main types of contract 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 of one to three years.

Pricing lists for cloud service 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 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. They 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 programmes, 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, in particular 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 involve a cloud service provider charging fees for the transfer of a certain amount of data outside of its environment and cloud infrastructure. They are called egress fees.

E. LEGISLATIVE AND REGULATORY CONTEXT

171. Several recent or pending European regulations and a national draft law containing transitional provisions specifically target the cloud sector.

1. THE DIGITAL MARKETS ACT

172. The Digital Market Act ("DMA"), adopted on 14 September 2022, is an asymmetric *ex ante* regulation of providers of "*essential platform services*", referred to as "*gatekeepers*", including "*cloud computing services*" (Article 2 (i)).

173. The obligations and prohibitions set out in Articles 5 and 6 of this regulation therefore apply to essential platform services provided or offered by gatekeepers[172] to user companies established in the European Union or to end-users established or located in the European Union, provided that these services constitute "*an important access point for business users to reach end-users*"[173]. These services will be expressly designated by the Commission for each gatekeeper.

174. If hyperscalers are designated as gatekeepers by the Commission and their cloud services are covered by the Commission's designation decisions, the DMA appears to impose limited obligations on them compared to the proposed Data Act discussed below. In fact, the DMA does not include any obligations aimed specifically at cloud services. In general terms, it provides for the following obligations that could apply in the cloud sector, in particular:

    - a ban on combining personal data from a core platform service with data from any other services, unless users give their consent (Article 5(2));
    - a ban on requiring business users or end users to subscribe to, or register with, any further core platform services as a condition for being able to use, access, sign up for or register with any of that gatekeeper's core platform services (Article 5(8));
    - a ban on using data generated by business users (Article 6(2));
    - an obligation for gatekeepers to provide the effective portability of data by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service (Article 6(9));
    - an obligation to provide business users, free of charge, with continuous and real-time access to the data provided for or generated in the context of the use of the relevant core platform services (Article 6(10)).

175. A gatekeeper shall inform the Commission of any intended concentration, where the merging entities or the target of concentration provide core platform services or any other services in the digital sector or enable the collection of data, irrespective of whether it is notifiable to the Commission (Article 14).

176. The Commission will designate the first gatekeepers from June 2023, and the obligations will apply to them from December 2023[174].

2. THE PROPOSED DATA ACT

177. The aim of the proposed Data Act is to ensure the better allocation of value from the use of personal and non-personal data among actors in the data economy. In particular, it

[172] As defined in Article 3 of the DMA.

[173] Article 3 of the DMA.

[174] https://www.entreprises.gouv.fr/fr/actualites/numerique/politique-numerique/adoption-de-la-legislation-sur-marches-numeriques-dma.

supplements the scope of the DMA by imposing minimum regulatory requirements of contractual, commercial and technical nature on cloud service providers to enable switching from one service to another.

178. The Commission's initial proposal of 23 February 2022 allows for:

- the portability of data, applications and "*other digital assets*" by guaranteeing functional equivalence between the same two types of services[175] when switching to another provider (Article 23);
- a withdrawal, after a transitional period of three years, of switching charges from providers (in addition to the egress fees already mentioned, these fees may include, for example, the cost of accompanying the customer to another cloud service provider) (Article 25(1));
- technical measures to make it easier to switch provider. For IaaS services, functional equivalence must be guaranteed, while for PaaS and SaaS services, providers must make "*open interfaces*" available to the public free of charge and comply with open interoperability specifications or European interoperability standards. In the absence of such standards, the cloud service provider " *shall, at the request of the customer, export all data generated or co-generated*", in a structured, commonly used and machine-readable format (Article 26);
- safeguards against illicit international access to non-personal data (Chapter VII);
- interoperability provisions are also set out in Chapter VIII. In particular, the Commission may request or more European organisations to draft European standards applicable to specific service types of data processing services (Article 29);
- the designation by Member States of one or more competent authorities responsible for the application and enforcement of the future regulation. In particular, the competent authority will be responsible for dealing with claims relating to the rights opened up by the regulation, without prejudice to any other administrative or jurisdictional remedy. A system of effective, proportionate and dissuasive sanctions may also be introduced.

179. The trialogue on the text began on 29 March 2023 and ended on 27 June.

3. THE DRAFT LAW TO SECURE AND REGULATE THE DIGITAL SPACE

180. The draft law includes several articles concerning the cloud sector:

- Article 7 provides a framework on transfer fees and cloud computing assets;
- Article 8 aims to ensure that cloud service providers comply with important interoperability and portability requirements where the same types of services are concerned. It also provides for the free availability to users and third-party service providers of interfaces and detailed information enabling the implementation of interoperability and portability requirements, as well as the publication and updating of interoperability technical reference offers. There are also plans to entrust the French telecom authority Arcep with the adoption of standards and technical specifications

[175] The Commission's proposal defines "*service type*" as "*a set of data processing services that share the same primary objective and basic data processing service model*" (Article 2(13)).

to promote competition in the sector, and more generally with the monitoring of this article, including through powers of investigation and sanction.

181. Referred to by the Government on this draft law, the *Autorité* issued Opinion 23-A-05 on 20 April 2023[176], making a number of recommendations aimed, in essence, at focusing interoperability obligations on the IaaS layer, distinguishing cloud credits according to whether they correspond to trial offers or longer-term support offers, clarifying data transfer fees and ensuring that the planned measures are properly coordinated with the future European framework, so as not to penalise operators operating in the French market.

4. OTHER REGULATORY FRAMEWORKS

182. Other regulatory developments, at both national and European level, also concern the management of cloud-related activities in terms of security, personal data protection and sovereignty. Some sector-specific regulations, for example in the financial, health or mobility sectors, also take cloud-related issues into account.

Legislative and regulatory context

This opinion is part of a wider and abundant regulatory environment, with in particular the 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 of 10 May 2023 to secure and regulate the digital space also includes provisions relating to the cloud.

II. How the sector works

183. Against a backdrop of rapid change in the public cloud sector, marked by significant technological innovation and strong growth momentum, cloud service providers can enjoy advantages linked to several market characteristics (A), differentiation through cloud products and services (B), cloud ecosystems (C) and their conglomerate structures (D). These characteristics can have an effect on competition and the market power of certain players, notably by creating barriers to entry and expansion. Competitive dynamics are presented in the final part (E).

A. MARKET CHARACTERISTICS

184. This section looks in detail at the various inputs required to provide cloud services (1) and the importance of critical size, given the high fixed costs and economies of scale and scope, which can act as barriers to entry and expansion (2).

[176] Opinion 23-A-05 of 20 April 2023 on the draft law to secure and regulate the digital space (link);

1. THE INPUTS NEEDED TO DELIVER CLOUD SERVICES

185. The provision of public cloud products and services requires several types of resources, which can represent significant costs and investments. According to one provider, "*the lion's share of the costs involved in providing a cloud service are linked to the rental or purchase of servers and server rooms, the supply of energy, technology licences, and payroll*". These different inputs are presented below.

a) Data centres and infrastructure requirements

186. As seen above (Part I), the provision of cloud services initially relies on physical infrastructures hosted in data centres. These inputs are essential elements that providers can acquire in a variety of ways.

187. The data centres needed to host the servers of cloud service providers may be built in-house, leased or outsourced to specialised service providers. The possibility of leasing or outsourcing can considerably reduce the barriers to market entry and expansion, given both data centre construction costs and the associated lead times.

188. These centres are particularly costly infrastructures. Based on the information collected during the investigation, the investment required to build a dedicated data centre is estimated at between 500 and 700 million euros. These costs include building construction, infrastructure equipment, and data centre design and layout. However, they can vary considerably depending on location, surface area, layout, etc. For example, according to one specialist, a small-scale data centre project can cost as little as 100 million euros, while the cost of building the largest centres can run from 700 million to 1 billion euros.

189. In addition to the financial implications, most of the companies surveyed emphasised the incompressible construction times involved. These timescales include land acquisition (identification of land, discussions with local and regional public authorities, obtaining permits), particularly in areas of high economic activity, as well as building construction and fitting out. On this last point, a number of players reported difficulties in obtaining certain equipment, against a backdrop of shortages or difficulties in sourcing some IT components. These steps also require the recruitment and training of profiles with rare skills. The investigation showed that the entire data centre construction project could take five to six years in France.

190. Given these costs and lead times, and the fact that data centres are infrastructures with relatively homogeneous characteristics, investment in and management of data centres are generally handled by a limited number of specialised service providers. A player like Equinix operates some 250 data centres worldwide, including ten in France, and plans to invest around €1 billion in France over the next five years to expand its capacity[177]. Given the scale of these investments, the market remains highly concentrated, with only a limited number of specialist providers able to meet the needs of cloud service providers and companies alike[178].

[177] BFMBusiness, "Choose France: American data centre specialist Equinix to invest €1 billion in France", 17 January 2022 (link).

[178] See BFMBusiness article cited above, according to the Managing Director of Equinix France, Equinix hosts 83% of CAC40 companies in its data centres.

191. According to the information collected during the investigation, most cloud service providers have favoured the use of specialist players, at least initially, to facilitate and accelerate their development in cloud services. For example, AWS currently has no data centres of its own in France. Google leased space in third-party data centres to run its services, before investing in its own data centres[179]. The same applies for OVHcloud, which began its business by renting data centres, before developing its own infrastructures. The investigation showed that when the major providers decide to develop their own data centres, their aim is to cover their own needs, which are already very substantial. These data centres generally have specific characteristics, such as a larger size and greater energy capacity, ensuring their owners lasting independence in a given region.

192. Even if they have not invested in their own data centres, cloud service providers still incur the operational costs associated with leasing data centre space. Pricing for these services includes location (rack space where the customer will place its servers, or more secure locations), power consumption, connectivity, and remuneration for specialised data centre personnel. These operating costs can be very high. According to one study[180], they account for 80% of cloud service providers' total costs (including energy costs). The average recurring cost of a data centre would be over 4.5 million euros per year and could reach over 7.5 million euros for large centres.

193. In addition to the data centres themselves, the significant costs involved in starting up and running services (servers, storage units, networks and infrastructure interconnections, etc.) are also an unavoidable expense for infrastructure service providers. Some equipment is subject to frequent renewal. As far as the network is concerned, to guarantee performance and ensure resilience and low latency, cloud infrastructures need to be connected as close as possible to the customer, with replication zones (usually three). In addition, intercontinental providers, particularly hyperscalers, deploy submarine cables to ensure data transfer between their different infrastructures located on different continents.

194. All in all, according to data provided by one hyperscaler, investment in buildings, land and physical infrastructure such as servers and other network equipment could account for almost 30% of the total network costs[181] of a major cloud service provider in France[182]. Operating expenses related to monitoring, power, cooling, maintenance and labour account for almost 70% of this cost.

b) Access to the technology and skills needed to develop services

195. In addition to the physical and IT infrastructures required to run cloud services, providers also face the costs of accessing the technology. While some technological building blocks, particularly for IaaS services, may be available as open source, others require licensing or the development of proprietary software solutions to create a set of functional services. Some technological solutions are indispensable and require constant updating and innovation. Several players also stressed the need to invest in security and compliance, so that customers

[179] Google Cloud France announced the opening of a Google Cloud region in France on 30 June 2022 (link).

[180] Emerson Network Power and Ponemon Institute study from 2016 (Emerson & Ponemon Institute, "Cost to Support Compute Capacity", 2016), taken up by the Dutch Competition Authority in its market study (ACM, Market Study Cloud service, 5 September 2022, p. 43 (link)).

[181] More on network costs in Part IV.A on egress fees.

[182] Calculations carried out by the investigation services on the basis of amounts communicated by a hyperscaler. These amounts are unaudited.

can be "*confident that their data and working environments are protected from unauthorised access*".

196. Generally speaking, the provision of cloud services involves large numbers of specialised human resources to create and deploy solutions and manage all the infrastructure (servers and networks) and solutions offered directly to the customer in the form of services. According to one hyperscaler, to provide a competitive offering, "*it is highly advisable to acquire skills in areas such as software deployment, information systems management, data analysis, application development, networking, security and systems architecture*". While these skills correspond to existing training courses at universities and engineering schools, their supply is limited and therefore costly.

197. Lastly, a number of providers reported a significant variation in technology access and development costs, depending on the range of services (functional depth) offered to customers. One hyperscaler pointed out that "*there are far fewer development costs when you only offer IaaS*". Services with higher added value for the customer require a wider range of services, as well as more resources, which are more costly, and a greater capacity for innovation.

2. THE IMPORTANCE OF CRITICAL SIZE

a) High fixed costs

198. One key feature of the public cloud business is the need to build a sufficiently large infrastructure before acquiring customers. The investments have to be made right from the start, and the return on investment, subject to the realisation of scale effects, takes time. At all times, the size of the infrastructure must be sized to meet the potential peak demand of customers contracting with the provider. Indeed, the customer must always be able to adapt its demand, either downwards or upwards. According to one hyperscaler, this requires sufficient resources from the outset to serve needs that are well above actual demand.

199. However, a large proportion of technological investment required to develop and operate a range of cloud services must be made upstream of commercialisation, particularly in the case of infrastructure services (IaaS). The use of specialised data centre leasing companies, which can help to gradually increase the size of the infrastructure as customers are acquired, can only partially reduces these initial investments.

200. Generally speaking, it is difficult to estimate precisely the total investment required to launch a viable offering on the market, as companies' development strategies have a considerable impact on the amounts involved. One company estimated that, in the French market, "*the minimum capital required to develop a cloud solution from scratch is around 100 to 200 million euros* [...]. *This includes human resources, the purchase of machines and other infrastructure equipment, deployment of the solution, and various costs relating to providers such as software vendors*". The minimum time required to become profitable would also be relatively long, averaging between four and seven years according to several estimates.

201. The provision of PaaS services is also characterised by significant fixed costs, linked to the development of new solutions and the need to rely on underlying infrastructure services. However, several players consider these costs to be generally lower than in the IaaS layer, as new entrants can choose to create and deploy their solutions on infrastructure managed by a third party. These solutions may be offered by public cloud service providers, within their own ecosystem. Total fixed costs would then be lower for providers positioning

themselves directly on this type of service (without offering IaaS services), compared to providing all services on an integrated basis. All other things being equal, it may nevertheless be more difficult for a player providing PaaS-only services to be as competitive as integrated providers (see below).

202. Moreover, fixed costs vary widely depending on the envisaged services and strategies. For example, investments may be particularly high for a company wishing to market an offer widely, to any customer profile over a vast territory, compared with a company targeting a niche market and a specific category of customers in a limited geographical area. However, having a global offering may be necessary to win multinational customers wanting to be able to locate their various workloads as close as possible to their customers, and avoid having to manage different providers in different markets. In this case, a provider will have to cover all the additional costs of using data centres in different countries, offering solutions in several languages, and maintaining local sales forces.

b) Economies of scale

203. This business is characterised by significant economies of scale due to the high fixed costs involved in offering cloud services. Economies of scale correspond to the decrease in the unit cost of a product as production increases. As a result, an established player with substantial production capacity will have an advantage over new entrants or smaller players.

204. There are economies of scale at various levels in cloud services. Firstly, at the level of the data centre itself, on the one hand, increased activity can lead to an increase in the size of the centre, which in turn increases fixed costs, but also leads to lower unit costs thanks to energy saving gains (e.g. lower cooling costs), labour or security, for example. According to the above-mentioned study by Emerson Network Power and Ponemon Institute, the economies of scale present in every cost item of a hyperscaler are even greater for energy and operating costs. These factors may partly explain why hyperscalers investing in their own data centres generally build larger infrastructures than those available for rental.

205. On the other hand, owning several data centres also generates additional effects, such as the ability to reproduce the basic architecture of a data centre, or easier networking. The use of data centres can also be optimised with greater total capacity spread over several territories.

206. Generally speaking, the larger the customer base a provider has, the better it can optimise its resources. As infrastructures are designed to cope with peaks in demand, a broad and diversified customer portfolio enables large public cloud infrastructure providers to meet demand with lower investment. For example, an e-commerce site will require increased resources during the holiday season, while a food delivery application will require an increase in those resources throughout the year, at mealtimes.

207. As its customer base expands, a provider is also able to automate services and increase productivity. As a result, they have a lower total cost of ownership[183] of their infrastructure. One hyperscaler, for example, uses artificial intelligence to continuously optimise infrastructure investments and avoid building data centres that are too large for demand. In

[183] The total cost of ownership represents the overall cost of an asset (an IT system, for example) throughout its life cycle, taking into account its acquisition and operating costs in their various dimensions: hardware costs such as computers, network infrastructures, etc. or software such as the cost of licences, indirect costs such as maintenance, administration, user and administrator training, upgrades, technical support and recurring costs (consumables, electricity, rent, etc.).

its ongoing drive to reduce costs, AWS has also developed its own chips ("Graviton") for its Amazon Elastic Compute Cloud ("Amazon EC2") service and regularly launches new versions to improve performance[184].

208. Once a critical size has been reached, cloud service providers also enjoy other economies of scale, linked to equipment purchases for example. They can for example benefit from discounts with large purchase volumes. Furthermore, according to one provider, in a context of shortages of IT components, hyperscalers benefit from privileged access to certain equipment due to their large purchasing volumes.

209. For managed services[185], providers also benefit from significant economies of scale. The production of these software solutions is mainly based on fixed costs (access to technology, human resources, production tools, hardware, etc.). Once the solution has been developed, marginal costs are very low, or even virtually non-existent, as the number of users has little impact on production costs. As a result, the more the solution is marketed, the greater the profitability. Similarly, the more customers the provider already has for its other solutions, the greater the potential for adapted service solutions.

c) Economies of scope

210. In addition to economies of scale, cloud services are characterised by significant economies of scope. Economies of scope appear when a company can increase its output by producing different goods from the same factors. In the case of the public cloud, these economies of scope can be found at different levels.

211. First of all, IaaS comprises a set of services that are distinct from one another, but largely based on the same resources, particularly in terms of technical infrastructure (data centres, servers, etc.), and for which the technological building blocks can also be pooled. Similarly, at the PaaS level, while the services can be very varied, the resources acquired and the first developments made can be mobilised to offer more services at lower cost.

212. Furthermore, a presence at all levels of the value chain, from IaaS to PaaS, could also enable to benefit from synergies. In particular, the ability to leverage the technical infrastructures of IaaS layers would facilitate the development of PaaS services. A number of technical and technological resources and skills could be shared between these service levels. These economies of scope between different cloud services can drive provider integration (see C.1. below), subsequently reducing the scope for new entrants to develop competitive offerings.

213. In conclusion, these characteristics influence the competitive functioning of the market, as they favour established players who can generate higher profits. As a result, the importance of fixed costs and the presence of significant economies of scale and scope in the cloud sector favour the concentration of players.

214. These characteristics also create significant barriers to entry and expansion for less developed players, to the benefit of companies with a head start and critical mass in cloud activities, for example, or with a presence in various digital markets (see D. below).

[184] Information on AWS Graviton is available on the AWS website (link).

[185] "Managed services" refers to PaaS and SaaS services (as opposed to IaaS services).

B. DIFFERENTIATING CLOUD PRODUCTS AND SERVICES

215. The following sections look at how cloud service offerings can be differentiated on the basis of certain characteristics, and at the strategies that providers can develop to gain competitive advantages.

1. Differentiating IaaS services

216. As far as infrastructure services (IaaS) are concerned, the investigation revealed that products and services are relatively homogeneous, with limited scope for differentiation for a new entrant. Therefore, in theory,, competition would be based mainly on price, which could benefit established players who already benefit from economies of scale and scope.

217. Other differentiating factors, such as infrastructure location or environmental impact, can also be considered.

a) Infrastructure location

218. Firstly, some providers could claim competitive advantages in terms of infrastructure location, which could have an impact on service quality.

219. On the one hand, the investigation showed that infrastructure location can be an important factor in customer choice, given its impact on latency times. This sensitivity to latency can be particularly important in certain business sectors. According to one provider, "*the geographical location of data centres can be a differentiating factor, insofar as geographical coverage reduces latency times for data access. This dimension can be strategic for certain customers, particularly in e-commerce, the financial sector or gaming*."

220. Furthermore, for some customers, it may be important to use a provider with infrastructures all over the world. According to one provider, "*for companies with an international footprint, geographical reach means that workloads can be deployed and operated anywhere in the world with little additional cost*". As we saw earlier, the investment required to offer this type of service is particularly high, and providers must be able to recoup it from a large and diversified customer base.

221. The ability to provide services to customers in specific countries can also be a differentiating factor. The investigation revealed that several providers may find it difficult to offer services in certain geographical areas. According to one provider, "*some countries, such as China, practise a policy of national preference, preventing foreign players from doing business on their territory, even in the form of joint ventures. This has been the case since 2017 for cloud computing in China, which requires the use of a local cloud provider*." Such territorial barriers can, in turn, confer competitive advantages on providers of certain nationalities. Alibaba stands out for its ability to provide services to companies operating in the Chinese market.

222. In France, providers such as OVHcloud, Scaleway and 3DS Outscale can benefit from a certain competitive advantage, due to their nationality and their infrastructures mainly located in France. International providers are also increasingly developing differentiated offerings, providing local hosting. For example, Google recently announced the launch of six new cloud regions (Austria, Czech Republic, Greece, Norway, South Africa and

Sweden), with the aim of offering more local offerings[186]. Similarly, on 1 January 2023, Microsoft launched its "EU Data Boundary" programme, which enables customers to store and process their data within European borders, in particular for its Azure services[187]. Oracle has also designed offerings specifically to meet the challenges of digital sovereignty, with different options depending on the customer's needs.

b) Environmental impact

223. As we saw earlier, cloud services, and in particular the operation of data centres, require significant energy consumption and can have an environmental impact. For example, Amazon's planned data centre in Ile-de-France, with 15,000 m² of computer rooms - one of the five largest data centres in France - is expected to generate 83 megawatts[188] of power, resulting in heat and particulate emissions[189].

224. Given the environmental challenges, the differences in resource management and optimisation can be a differentiating factor between players. One cloud service provider considered that "*the differentiation of cloud offerings is based in particular on the consideration of energy efficiency and environmental impact in a context where customers (i) are facing rising energy costs, and (ii) are developing responsible purchasing policies*".

225. A number of providers are therefore seeking to highlight the energy performance of their services. For example, OVHcloud has developed its own water-based cooling system for its server rooms, eliminating the need for air conditioning[190]. Scaleway has also opened a data centre in the Paris region (DC5), equipped with a natural cooling system, known as adiabatic cooling, which saves around 40% in energy consumption compared with a conventional data centre[191]. Oracle says it uses 100% renewable energy to operate several of its cloud regions (notably the Paris region), with the aim of making this the case for all its cloud regions worldwide by 2025[192]. French company Qarnot specialises in the sale of high-performance computing systems that use IT waste heat[193]. Qarnot operates a shared computing infrastructure, in the form of computing clusters located in buildings and industrial facilities requiring heat.

226. On these subjects, the ability to differentiate between providers can be direct, if customer companies attach importance to this criterion.

[186] TechCrunch, "*Google Cloud expands to six more countries*", 11 October 2022 (link).

[187] Programme presentation on the Microsoft website (link).

[188] By way of comparison, 100 megawatts are equivalent to the electrical capacity of the Verbois dam in Switzerland (link).

[189] Le Journal du Net, "Exclu JDN: Amazon's secret data centre project in Ile-de-France revealed", updated on 18 October 2022 (link).

[190] L'usine nouvelle, "How does OVHcloud's data centre cooling system work?", 26 June 2019, updated on 10 March 2021 (link).

[191] 01net, "We visited DC5, Scaleway's data centre with its unique, eco-friendly cooling system", 6 June 2021 (link).

[192] Press release, "Oracle Reinforces Commitment to France by Opening a Second Cloud Region", 20 June 2021 (link).

[193] Waste heat is thermal energy produced indirectly by a process and neither recovered nor valorised.

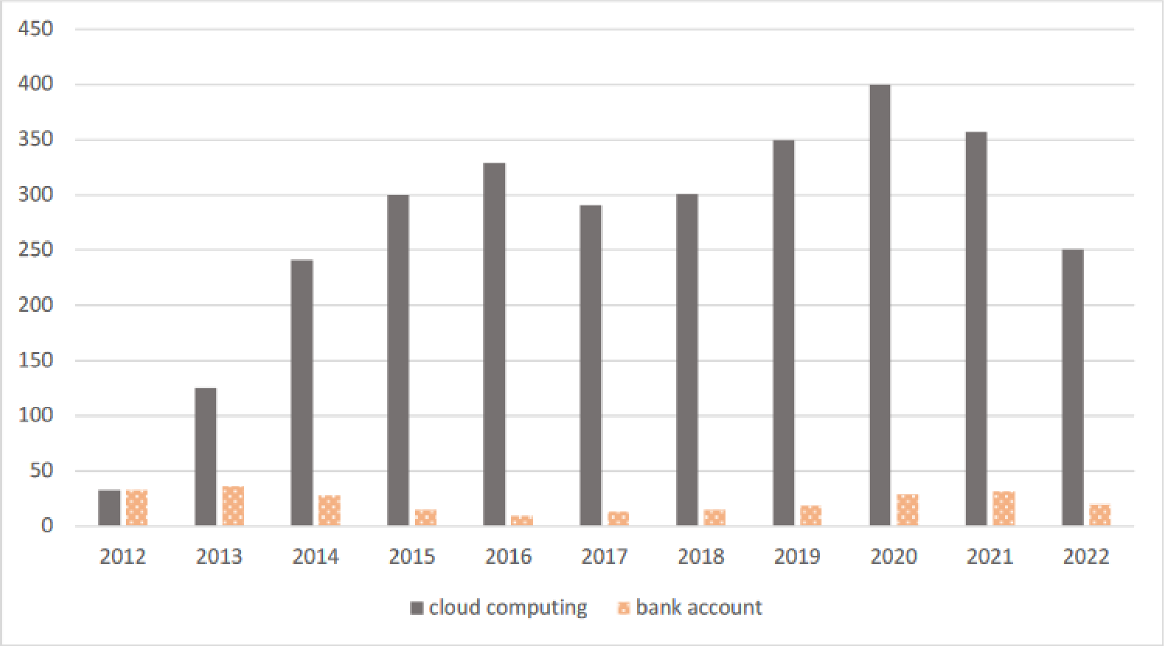
2. DIFFERENTIATION THROUGH MANAGED SERVICES (PAAS AND SAAS)

227. While differentiation capabilities may appear relatively limited in the IaaS sector, the investigation showed that providers generally try to differentiate themselves by offering value-added services to customers. Most major public cloud service providers currently provide both IaaS and additional managed services (such as PaaS or SaaS). For the moment, these services are less widely used than IaaS but are likely to facilitate the development of diversified offerings. Taken as a whole, cloud providers' offerings could therefore prove less homogeneous. Several main areas of service differentiation can be envisaged, based on the information collected.

a) Innovation

228. Generally speaking, the players emphasised the high level of innovation in the cloud market, which leaves room for many possible types of diversification. Some authors[194] pointed to the large number of patents filed in the United States in the cloud sector, compared with the banking sector.

Figure 14- Number of US patents for the cloud and banking sectors (2012-2022)



Source: United States Patent and Trademark Office (Sean Ennis and Ben Evans, Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence, 29 March 2023, page 10)

[194] Sean Ennis and Ben Evans, "*Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence*", 29 March 2023, page 10 (link). According to the authors, the comparison with the banking sector is justified since Open Banking is often held up as an example to explain the implementation of interoperability in the cloud sector. However, the characteristics of the two sectors differ, particularly in terms of the number of innovations. The term Open Banking describes a business model based on the use of APIs to share financial data between different parties. This includes data shared between financial service providers (banks, insurance companies, resellers, etc.), between providers and their customers, or between individuals (source: Red Hat, L'Open Banking, qu'est-ce que c'est?, 18 November 2022 (link)).

229. Managed services are considered by many providers to offer the greatest potential for innovation and new solutions. Cloud service providers are in the midst of a dynamic of innovation that is broadening the scope and capacity of their offerings to compete and to meet customer demand. By proposing new services (often referred to as "proprietary"[195]), bringing greater added value (better quality, greater security, etc.) or even new functionalities (for example, new artificial intelligence services), providers have multiple means of differentiation at their disposal. As a result, and given the lower barriers to entry, the potential for entry and development of players in these services appears higher than for IaaS services.

230. By way of example, a number of companies, such as Google and Scaleway (see Part IV), are looking to innovate in order to offer solutions that facilitate the use of multi-cloud, given not only customer interest but also the potential for opening up the market for less established service providers.

231. Players with the greatest capacity for innovation and the rapid development of new value-added services for customers, for example through economies of scope, can therefore benefit from significant competitive advantages.

b) Sector specialisation

232. Several players consider that it is also possible for cloud service providers to differentiate themselves by offering services that meet the specific needs of a particular type of company or sector. By way of example, one company indicated that the specific video streaming services offered by AWS were differentiating services, in view of its activities.

233. Some sectors, such as the healthcare or financial sector, have often been cited as having specific needs, given their highly regulated nature. However, the ability of providers to differentiate themselves by proposing specific offers for this type of sectors is perceived differently by different players.

234. Microsoft has made the strategic choice to offer sector-specific solutions, in the belief that customers demand solutions that correspond to their sector-specific needs. A "cloud for industry" offering has therefore been developed, bringing together solutions proposed by partners such as Sopra Steria (integrator and consulting company) to offer a bundled product tailored to the needs of different sectors (e.g. banking, healthcare, retail)[196].

235. However, Microsoft's offerings do not presuppose the future definition of relevant markets in the cloud sector, notably since, according to the investigation, there is currently no specific demand for cloud services dedicated to certain sectors (see Part III below). In addition, other providers see no need to develop specific offerings, since the same service can be useful to a wide range of customers, whatever the sector.

c) Quantity of services

236. The investigation showed that PaaS services are an important factor in the attractiveness of cloud service providers. In addition to the higher competitiveness of certain services, the

[195] "*In computing, proprietary software or services are owned by an organisation or individual, as opposed to "public domain" software (open source)*" (Gartner glossary, link).

[196] See, for example, the Microsoft website (link).

differentiation between providers is also based on the number of services offered in their catalogues.

237. The extent of the catalogue seems to be an important element in the choice of provider, as the customer will prefer the offer that covers all its current as well as future needs. Several companies reported that they had observed and taken into account the difference in catalogue breadth between service providers, even though their current actual usage covered only a limited portion of these services. One provider summed up this point by saying that, "*the provision of PaaS services enables customers to make significant savings in the costs of administering and maintaining hosted services. The ability to offer a wide range of services and an extensive catalogue is a key competitive advantage, as customers naturally gravitate towards a one-stop shop where they can find all the services they want in one place, with centralised invoicing and shared management of access rights for all the services they want to order. The more extensive a provider's catalogue, the more likely it is to become that one-stop shop for the cloud customer*".

238. Providers able to provide the most comprehensive catalogues would therefore be more attractive, enabling them to reach a large number of potential customers more quickly and benefit from scale effects. This situation would raise barriers to entry for new or more specialised players, who would be unable to offer a comparable product in the short term. The partnership approach enabled by the development of marketplaces can also contribute to the mutual enrichment of providers' offers.

3. Certifications and "trusted cloud" offers

a) Certifications

239. There are several certifications for cloud technologies and services. These certifications can attest to a certain level of quality and to compliance with certain conditions, such as those relating to security. Some may be cross-functional, such as those dealing with security issues (e.g. ISO 27001, ISO 27017, ISO 27018), or sector-specific, such as "HDS" certification. Obtaining these certifications can be a way for a provider to differentiate itself from its competitors, enabling it to claim a higher level of quality by giving it access to sectors for which certain certifications are required.

240. In addition, several providers pointed to the many different certifications which, taken together, make it possible to attract a large number of customers around the world, with requirements varying from country to country. This situation tends to reinforce barriers to entry and expansion and gives an advantage to multinational players, who have substantial development resources at their disposal to ensure compliance at all levels. Hyperscalers generally highlight their compliance status, as does Microsoft, which lists offers that comply with over 100 legal and regulatory standards for Azure on its website[197]. AWS also states on its website that its customers can "*inherit the most comprehensive compliance controls with AWS. AWS supports 143 security standards and compliance certifications*"[198].

b) "Trusted cloud" offerings and the SecNumCloud certification

[197] Microsoft site, Azure compliance documentation (link).

[198] AWS website, compliance (link).

241. The investigation showed that, of all the certifications or labels linked to cloud services, SecNumCloud certification is the most structured for the French market.

242. The majority of providers and customers considered that obtaining this certification, which is necessary to meet the demands of certain players to reinforce data protection or comply with regulatory obligations, opens up opportunities for differentiation between offers, and would therefore be likely to confer a certain market power to its beneficiaries, and create a barrier to entry at various levels.

243. On the one hand, some providers may not be able to meet the criteria due to their non-European nationality. One hyperscaler considered that this strategy has "*an immediate, significant and lasting effect on the competitive operation of the cloud market in France, as it excludes the cloud offerings of non-European cloud providers and hyperscalers from the French government's public calls for tender and the calls for tender of OVIs' critical information systems*". The entry into force of the "trusted cloud" strategy may well have jeopardised the plans of several non-European hyperscalers. For example, Microsoft had to abandon plans to adopt its solutions by the French Ministry of Education and Youth[199].

244. According to one hyperscaler, the effects extend beyond the players directly affected by the "cloud au centre” (cloud at the centre) strategy, with many companies preferring to turn to certified offerings "*by anticipation, political choice or misunderstanding of the doctrine*". Another provider also noted, "*since 2021, an irrationality in the market, involving asking 'by default' for trusted cloud, despite the absence of offers, for use cases that do not justify a high level of security*".

245. On the other hand, for other players who would not be excluded by the criteria set, certification would still entail barriers to entry, as the cost of the necessary adaptations to their offering would be too high. The requirements of the standard would necessitate a thorough overhaul of their existing services to make them compatible. On this subject, however, cloud service providers’ opinions are relatively divided. On the one hand, some consider that the investment required would be too high for the expected benefits. One provider testified that, given its size and the importance of devoting all its resources to maintaining a competitive offering vis-à-vis the biggest players on the market, it could not meet the requirements of the standard to gain access to the market of customers subject to the "cloud de confiance” (trusted cloud) strategy, unless it lost competitiveness more globally. On the other hand, some players believe that these investments are worth making, as they will pay for themselves in the future. Cloud Temple, for example, chose to mobilise an in-house team of 20 developers over a period of two and a half years to set up systems that meet the SecNumCloud certification criteria[200].

246. The profitability of the investments required could also be reassessed by certain players in view of the prospect of extending certification obligations to more customers. The government does not seem to have ruled out this possibility. In his 12 September 2022 speech on the national cloud strategy, Bruno Le Maire, Minister of the Economy, Finance and Industrial and Digital Sovereignty, declared, "*I say it with great gravity,, if ever our companies with extraordinarily sensitive data do not freely take up this offer to secure their*

[199] Zdnet, "*Microsoft must leave schools, confirms French Ministry of Education*", 18 November 2022 (link).

[200] Le Journal du Net, "*Cloud temple, the French sovereign cloud targeting Europe*", updated 2 November 2022 (link).

data, I cannot rule out that, at some point, we will introduce a mandatory standard to protect our industrial sovereignty and our independence"[201]. A broader compliance obligation could, however, have an impact on the market, with the risk of excluding certain providers experiencing compliance difficulties from a large part of the demand.

247. To overcome the barriers to entry, a number of partnership projects have emerged to provide a certified offering. The investigation revealed that this partnership dynamic elicits varying reactions from different players, particularly in the case of partnerships between American hyperscalers and European cloud service providers or integrators. Many customers believe that such groupings can make the offers of European providers more attractive. Conversely, several providers considered that although these offerings do not really guarantee protection against the application of foreign laws, they allow US hyperscalers to maintain their advantages, rather than offering opportunities to regional cloud service providers. One provider considered that "*major buyers only expect the 'same' version in the form of a joint-venture (e.g. Bleu)*".

248. Without calling into question the criteria set out in the standard, the *Autorité* points out that excessive barriers to entry can give rise to competitive risks, which would be even higher if the obligation to comply extended beyond the players currently targeted by the "cloud at the centre" strategy.

249. In this respect, aids such as the qualification support scheme announced by the Government[202], can be an appropriate response. This scheme, with a budget of 3.5 million euro was launched on 22 December 2022 and entrusted to BpiFrance. It targets primarily SMEs wanting to market a SecNumCloud-qualified offering within two years[203]. Some companies may also be positioned to support providers. For example, 3DS Outscale, in partnership with ANSSI, has launched a "Path to a trusted Cloud" programme to help software vendors obtain SecNumCloud qualification by providing feedback and best practices, as well as qualified IaaS services on which to build their services[204].

250. It should be noted that a similar situation is expected with the introduction of the European Cybersecurity Certification Scheme for cloud service providers, the EUCS (see above). Several Member States have expressed their opposition to an overly restrictive scheme that could penalise SMEs. The same applies to some international cloud players, who, in a statement published on 2 December 2022[205], highlighted the risk of certain providers being excluded from the market, particularly in view of the extraterritorial immunity criteria.

251. For some of the players interviewed, however, this European certification may also have positive effects in terms of competition, compared to the current fragmentation of the European market due to the proliferation of national certifications, which, according to the investigation, can make it more difficult to choose providers.

[201] Speech by Bruno Le Maire on the national cloud strategy, 12 September 2022 in Strasbourg (link).

[202] Ministry of the Economy, Finance and Industrial and Digital Sovereignty, "*Cloud: five new systems to support sector development*" (link).

[203] ANSSI website, "*Trusted cloud: new support system for obtaining SecNumCloud security authorisation for our startups and SMEs*", 22 December 2022 (link).

[204] 3DS Outscale website, "Path to a trusted Cloud: a major asset for SecNumCloud qualification", 26 January 2023 (link).

[205] See the press release here.

C. THE BENEFITS OF CLOUD ECOSYSTEMS

252. An analysis of the way the sector operates, and the positioning of the different players, tends to show that some providers are building cloud ecosystems, i.e. a set of integrated services that customers can access, including the provider's proprietary services, but also, generally through marketplaces, a set of services from third-party developers, designed to operate within this ecosystem. The industry could therefore be structured around competition between cloud ecosystems.

1. SERVICE INTEGRATION

253. The analysis of the cloud sector showed that the main cloud service providers are present at different levels of the value chain, particularly in IaaS and PaaS services, and offer integrated packages covering these different service levels. Hyperscalers provide a service integrating a set of underlying services managed in-house and working closely with their other services. In fact, one hyperscaler pointed out that "*solutions are not designed to operate on generic hardware, but are specifically tailored to operate in an environment tightly managed by the provider*".

254. In this way, infrastructures are designed and scaled by the provider to meet its needs. Similarly, the whole technology stack[206] for PaaS infrastructures (see paragraphs 372 et seq. below) is specifically designed to optimise operation across the provider's entire network (moving workloads, managing updates, patches, etc.).

255. While it may be difficult for new entrants to compete effectively with large, integrated companies, there are certain advantages for the customer, who can purchase the services required for their business without having to manage all their IT needs or worry about the technical difficulties of interoperability, all without interconnection costs.

256. Providing integrated solutions also enables providers to offer solutions that cover all customer needs, and therefore generate greater revenues and economies of scale and scope (see Part II.A.). According to the information collected during the investigation, traditional IaaS services, in particular compute and storage services, are still the biggest source of revenue and investment for cloud service providers. These services are also an essential component of PaaS, and therefore benefit from the development of PaaS activities for integrated providers. Furthermore, providers who also offer PaaS services are also benefiting from the attractiveness of these services to earn more revenue in this segment.

257. According to the information collected, integrated providers as a whole are seeing a significant increase in the percentage of PaaS services in their total revenues. One hyperscaler, for example, has seen the proportion of its revenues in France generated by PaaS rise from 25% in 2019 to 42% in 2021[207]. According to several providers with a long history in IaaS, PaaS is a strategic area in which to increase revenues, due to the added value it offers customers. One provider, for example, reported that PaaS accounts for more than

[206] The products that make up a company's IT installation (or technology stack) consist of a set of layers constituting, as the Commission noted, the "*consists of the various hardware and software components necessary for companies to ultimately use business software applications*" (Case COMP/M.5529, Oracle/Sun Microsystems, footnote 6, page 9).

[207] Calculations by the Autorité de la concurrence on the basis of the information collected.

half of its recent recruitments, even though it still represents a limited amount of its total turnover.

2. ACCESS TO THIRD-PARTY SERVICES

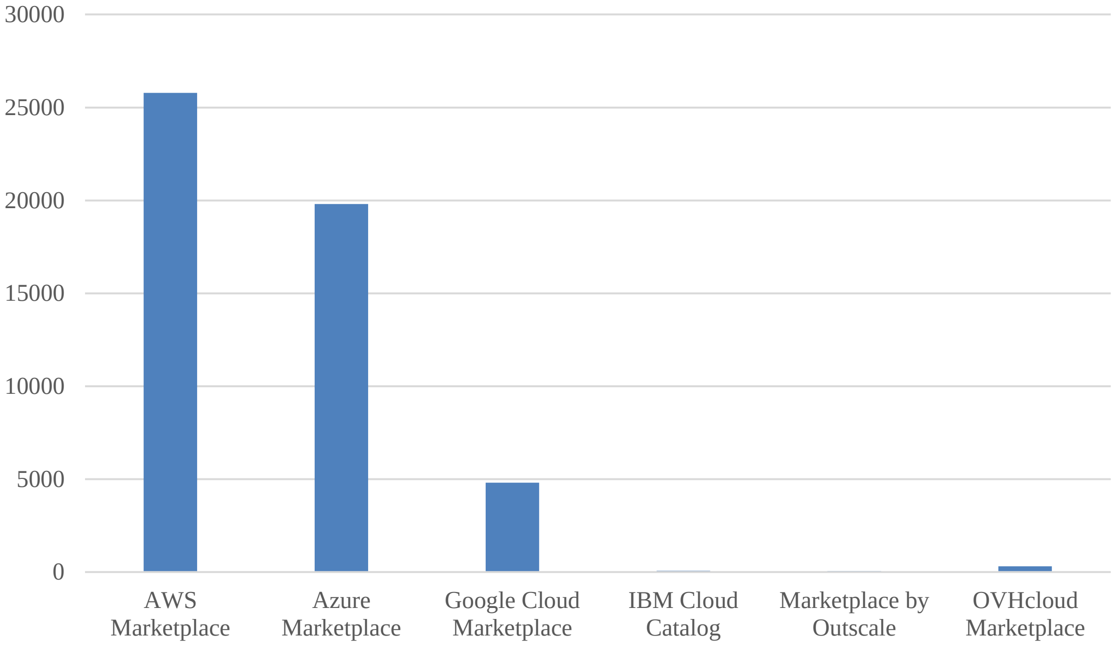
258. In addition to integration, the major providers tend to build ecosystems in which the customer can access all the provider's proprietary services, as well as third-party services designed to operate within their ecosystem. These third-party services may be accessible via a marketplace made available by the provider itself.

259. As seen earlier (see B. above), the quantity of services available is an important factor in a customer's choice of provider. In this way, a provider can be encouraged to open up its ecosystem to third parties, in order to increase the number of services available and provide access to certain services that are particularly in demand. One provider stated that "*the depth of a marketplace's catalogue, like the number of software products available on a platform like Android (Google) or IoS (Apple), is a decisive factor in customers' choice. In IT, it is always the use cases, and therefore the applications, that have generated the uses of hardware platforms. Cloud offerings with the greatest catalogue depth, as well as "killer apps" and must-have applications, are highly favoured by customer*s".

260. The dynamic corresponds to that of indirect network effects between two categories of players, in this case customers and third-party developers. From this point of view, an ecosystem (see 4. below) will be even more attractive to customers the more services operating in the cloud environment are offered, while developers will also be more encouraged to propose suitable solutions the more they can offer them to a broad customer base. This dynamic tends to strengthen the position of providers who have succeeded in reaching a significant size (ideally on both sides of the market, but at the very least on one of them) and reinforces the barriers to entry and development.

261. The data collected by the investigation services seems consistent with such a dynamic. As shown in the graph below (see Figure 15), the leading providers in terms of revenues and customers both worldwide and in France are also those who offer the largest number of third-party services on their marketplaces. The differences are particularly significant, with AWS having more than five times as many third-party services on its marketplace than Google Cloud in November 2022.

Figure 15 - Number of third-party services offered on cloud service providers' marketplaces



Source: marketplace websites, data collected on 4 November 2022.

262. It should be noted, however, that marketplaces are not the only way to open up ecosystems to third-party solutions. The investigation revealed that third-party developers currently use multiple distribution channels, such as direct sales or independent intermediaries.

263. However, a marketplace is a particularly interesting tool, and the majority of integrated cloud service providers have created their own in recent years. From the customer's point of view, marketplaces provide access to a wide range of products and services on a single interface, reducing search costs. They also offer an easy-to-implement contractual framework. At the same time, with regards to third-party developers, several players consider that marketplaces are a very useful way of accessing large customer bases, which would otherwise have been costly to reach. So, according to one hyperscaler, selling through its marketplace "*offers third-party providers security in terms of payment receipt, and provides an easy-to-use channel for distributing and installing products in a cloud environment, as well as for providing update services and patching products*".

264. However, these benefits may be more limited in the case of solutions that already benefit from a solid reputation and a substantial installed base. Developers may then have an incentive to use this market power to limit third-party access to their solutions, in order to reduce the attractiveness of these third parties. In this respect, it is worth noting that solutions from large integrated providers are generally not offered or accessible in other ecosystems, as these providers reserve them for their own.

265. In addition to marketplaces, the ecosystems of different cloud providers can be more or less open, depending on whether the technical and contractual characteristics of their products allow interoperability or multi-cloud use. Strategies can vary according to providers and their market position, creating different incentives to open up their ecosystems. According to one hyperscaler, "*services that enable users to adopt a multi-cloud strategy, for example by being open and interoperable with third-party services, are likely to be more attractive to customers*". However, the investigation showed that some hyperscalers are tending to

develop strategies that limit the openness of their ecosystem, notably through barriers to interoperability (see Part IV).

3. NETWORK EFFECTS

266. Due to the specific nature of cloud products and services (particularly PaaS), there are significant learning costs, and a *de facto* incentive for developers to focus on learning the most widely used and most in-demand solutions. This creates beneficial network effects for the latter, with learning costs amplifying these effects. Information collected during the course of the investigation indicated that this dynamic is largely maintained by an active approach on the part of hyperscalers, aimed at encouraging developers to learn their solutions and, consequently, win their loyalty. This includes dedicated training courses at developer schools. Some even have their own training programmes, like Microsoft, which has created several "schools" in partnership with the Simplon school[208]. Several smaller providers do not believe they have the capacity to develop these strategies, given the resources required to build up a network of trainers and approach partner schools.

267. Hyperscalers also generally offer certification programmes for professionals, some of which are free of charge. These programmes include online training and an exam (online or at an exam centre). These certifications can usually be accessed directly on the provider's website[209]. Microsoft[210], for example, offers over 70 Azure certifications and exams. These certifications, which focus on the use of the provider's solutions, attest to the skills that recruiters are looking for and are therefore particularly valuable for professionals[211].

268. Overall, these network effects help to strengthen the position of the main ecosystems to the detriment of other providers. According to one provider, "*the brand image of hyperscaler has become a sesame for developers, who have pounced on certifications that add value to their profiles. This creates a turnover of skills and drives up salaries. This situation drains other technologies, which do not enjoy the same level of notoriety and fail to interest Cloud developers and architects due to a lack of value. As a result, customers turn to the skills most present on the market, also fuelling the race for salaries and technological skills. These factors favour hyperscalers*."

269. In this way, the availability of profiles trained in an ecosystem, whether employed directly or through subcontractors, helps to reinforce the attractiveness of a cloud provider. Several customers heard during the investigation confirmed that they had taken this aspect into account in their choice. At the same time, integrators, who can advise customers and steer them towards certain technologies as a priority, may also have an interest in favouring the technologies most widely used and mastered by their developers. The 2020 report by the Antitrust Subcommittee of the U.S. House of Representatives also noted this dynamic, which was helping to give AWS, the market leader in the U.S., a significant competitive edge: "[*t*]*he widespread adoption of AWS's developer certification programs, partner networks, and student programs means that there are more engineers familiar with AWS technology*

[208] Microsoft website, "*Microsoft France inaugurates the third Microsoft by Simplon AI School with La Manufacture des Talents Michelin in Clermont-Ferrand*", 16 November 2022 (link).

[209] AWS website, Training and certification (link). Google Cloud website, Google Cloud Certification (link).

[210]Microsoft website, Azure Certification (link).

[211] Le Point, "Ongoing training - When the GAFAM get involved", 25 May 2022 (link).

than with any other platform. Several market participants listed the availability of AWS-trained engineers as a reason for selecting AWS over other cloud providers and as a barrier to migration to another platform or multi-cloud adoption"[212].

4. Competition between ecosystems

270. Competition between ecosystems is characterised by potentially limited competition *in* the market once relationships have been established (a) and competition *for* the market (b).

a) Potentially limited competition *in* the market once relationships have been established

271. The barriers to migration can be particularly high for workloads that relies on ecosystem-specific services, not least due to the limited substitutability between ecosystems. Indeed, as it has already been seen (see 1 above), each ecosystem is based on a set of solutions and integration schemes that are difficult for a competitor to reproduce.

272. Once the customer has been captured by the primary provider, it is very difficult for them to migrate their workloads to another competing provider, especially when it comes to PaaS services. Indeed, while some of the individual services offered within ecosystems are experiencing a form of standardisation, particularly within infrastructure services (IaaS)[213], the investigation showed that there are particularly significant differences between the most recent and innovative services, particularly in PaaS, and providers' proprietary services (see Part II.B). One hyperscaler confirmed that, "*the newer, more recent and potentially unique the functionalities implemented, the less standardised they are*".

273. In addition, the integration of different services, particularly IaaS and PaaS, to meet the customer's needs, makes the entire service provided at the workload level specific to an ecosystem, and therefore all the more difficult for competitors to replicate (see Part IV). These barriers to migration, linked to the integration of services, also work against the implementation of a multi-homing strategy within the workload, whereby only part of the services are migrated to another provider. One customer confirmed that "*the integration of certain services from certain providers can also be a major obstacle to multi-cloud, as these services are specific to a single operator, and particularly to the customer*".

274. Differences between ecosystems also mean high learning costs for customers in the event of a migration project. In this case, customers have to learn how to use new ecosystems, and the time required to train or recruit new profiles must be taken into account (see 3 above). As one hyperscaler put it: "*each public cloud has a slightly different architecture and a slightly different management portal and user interface. As a result, there is a learning curve for IT professionals managing different cloud services. If a company wants to move a workload from one public cloud to another, the IT professional in charge must learn how to use the new cloud's interfaces. This can take time and effort, depending on the number of IT professionals involved*." As a result, many of the investments initially made by the company

[212] US House of Representatives Sub-Committee on Antitrust, Investigation of competition in digital markets, 2020, p. 269 (link).

[213] As mentioned above, a number of industry players talk in terms of "*convenience*", although it should be noted that some of the players interviewed considered that there are still technical obstacles to migrating IaaS workloads to another provider.

to integrate the first provider's solutions (technical integration costs, training, etc.) would be sunk costs for the customer, and would therefore act as a disincentive to migration.

275. It is clear from the above that migrating a workload to another ecosystem represents a major investment in terms of time and resources. By using the services of an ecosystem for one or more workloads, the customer is making a choice that structures the organisation of its IT system and commits it for many years to come. This situation strongly limits competitive pressure from other providers, even if they are part of ecosystems, and gives the chosen primary provider considerable market power.

276. All in all, the integration of services and the creation of ecosystems create multiple barriers to entry for new providers, as well as barriers to expansion for providers present in only one part of the market. In addition, some providers may take deliberate actions to attract and lock in their customers (see Part IV).

b) Competition *for* the market

277. In a situation of competition *for* the market, the main ecosystems seek to win over customers when they choose their first cloud provider ("primary-provider") for one or more workloads. While, as seen in Part I, the customer can use a multi-cloud strategy, the investigation revealed that in the vast majority of cases this is implemented in silos, i.e. the customer uses several providers but for separate workloads, except for very specific needs.

278. When faced with a given need or workload, customers - whether migrating to the cloud or cloud-native - are encouraged to use a single provider capable of meeting all their needs. There are several advantages to using a single provider for a single workload, or even for several workloads if they are linked. In particular, the customer avoids many of the difficulties associated with managing interoperability between services from different providers as well as the complexity of using different solutions simultaneously (see Part I.B.4). These difficulties are generally the source of additional costs and also introduce technical risks into projects, particularly in terms of security or delays in service delivery. The use of multi-cloud also forces the customer to take on more operational responsibilities. According to one cloud service provider, the integration of a provider's services is a major obstacle to multi-cloud, because "*it is always easier to use automation tools to move data from one process to another within the same provider, rather than having to export this data in a standard format so that it can be reused by another provider*".

279. From this perspective, large hyperscalers organised into ecosystems benefit from competitive advantages over providers offering less extensive solutions, and competitive bidding will generally lead to the selection of a provider who will cover the customer's entire need (specific workload(s)), which is akin to competition *for* the market. These advantages can also be reinforced by certain behaviours on the part of the provider, leading the customer to entrust it with all their needs (see Part IV).

280. This situation, in which the provider satisfies all the customer's needs and where it is very difficult to change provider, increases the barriers to entry and expansion for a provider who cannot gradually win over the customer of another provider. Competition will therefore tend to concentrate around the main ecosystems, particularly for workloads requiring a wide range of cloud services.

D. CONGLOMERATE ADVANTAGES

281. The well-established position of certain players in digital markets outside the cloud could give rise to a range of competitive advantages of a conglomerate nature.

1. THE IMMENSE FINANCIAL CAPABILITIES OF CERTAIN PROVIDERS

282. Firstly, the investigation revealed that many players believe that companies with strong positions in other digital segments benefit greatly from their substantial financing capacity to invest in cloud services.

283. Quantifying the investments made by the market's leading providers has proved difficult. Most public information and financial data are aggregated both by investment item and by geographical area. However, the information collected during the investigation points to very high investment capacities among the major digital players, in the order of several billion euros worldwide[214], with investments by other providers generally ranging from a few million to a few hundred million euros.

284. Large digital companies also seem able to withstand cumulative losses over several years as part of their market conquest strategy. By way of illustration, according to Gartner[215], despite its revenue growth and significant market share, Google Cloud has experienced losses from its inception in 2018 through to 2022 (see Part I.C). Such a situation appeared tenable in view of the Group's worldwide margins. This aspect was emphasised by many providers, who saw it as creating a very significant competitive advantage for the major digital players over specialised players.

285. These investment capacities also take the form of external growth through company acquisitions. The investigation showed that the major digital companies have been buying up a large number of cloud companies in recent years, whereas such takeovers are rare among pure players (see V.C.). Merger operations).

2. ECONOMIES OF SCALE AND SCOPE WITHIN THE CONGLOMERATE

286. In addition to the economies of scale and scope (see A.2 above) intrinsic to cloud services, conglomerates can enjoy economies of scale and scope linked to their different activities.

287. Firstly, unlike pure cloud service providers, large digital service providers have benefited from the critical mass conferred by their own internal needs ever since the launch of their cloud activities. AWS launched its first public cloud service offerings to monetise the investments it had made in infrastructure of sufficient size to support its own e-commerce service activity peaks. Similarly, other major digital players have entered the public cloud services business after investing for their own needs. Furthermore, the cloud capabilities deployed within a diverse conglomerate can be used for a wide variety of activities, such as web applications, video streaming, search engine services or the Internet of Things.

[214] For example, in April 2020 Alibaba Cloud announced that it would be investing nearly 26 billion euros over the next three years to develop Alibaba Cloud's infrastructure and cloud-related technologies (link). For the French market alone, AWS is planning a total investment of 6 billion euros over the period 2017-2031 (link).

[215] Gartner, Magic Quadrant for Cloud Infrastructure and Platform Services, published on 19 October 2022.

288. In addition, through their other related activities, the major digital players already had numerous advantages, particularly in terms of economies of scope, for deploying services in the cloud. Several skills and technological building blocks already developed have been used to offer cloud services in their ecosystem, for example in terms of database management, artificial intelligence or marketing. These technical synergies have enabled these players to offer attractive products at lower cost. More generally, the R&D work of these conglomerates has benefited from a range of activities within the conglomerate.

289. Last but not least, providers historically established in software product markets (on-premise) seem to have specific advantages. They have an established customer base, and are well known among the companies that use their products on-premise. These historic positions have been used as leverage to develop their cloud offerings.

3. Customer acquisition by hyperscalers

290. Several factors combine to make customers captive to the hyperscalers present in different digital sectors: difficulty in migrating from one hyperscaler to another, poor interoperability between the services of these providers, and familiarity with the other tools and services offered by these providers.

291. The major digital players may appear more attractive to certain customers already used to their services in other markets, who therefore avoid the learning costs associated, for example, with changing tools or interfaces that are generally common or have significant similarities between the different services.

292. In addition, the investigation revealed that players present in multiple markets generally tend to integrate their different services, for example through unified connections between all the services offered (cloud and non-cloud) and the centralised management of cloud and non-cloud accounts, which would also help encourage customers to manage everything with a single provider.

293. The ability to offer a wide range of services enhances the attractiveness of these companies, enabling them to position themselves as strategic partners for supporting companies at different levels. Several partnerships have been announced in recent years. For example, in 2016, the Renault-Nissan Group entered into a partnership with Microsoft to make Azure the automotive group's platform for "*advanced navigation, predictive maintenance, vehicle-centric services, remote control of vehicle functions, external mobility and real-time updates*"[216]. Similarly, the LVMH Group entered into a partnership with Google Cloud to "*significantly improve operations in the areas of demand forecasting and inventory optimisation, and to take the customer experience to new levels, thanks in particular to ever greater personalisation*"[217]. Amazon entered into a partnership with Stellantis in 2022 to "*deploy Amazon's technology and software expertise across its organisation, including for vehicle development, creating connected on-board experiences and training the next generation of automotive software engineers. Together, the two companies will develop a*

[216] Les Echos, "Connected car: Renault-Nissan joins forces with Microsoft", 26 September 2016 (link).

[217] Press release of 16 June 2021, "LVMH and Google Cloud create strategic partnership for AI and cloud-based innovation" (link).

suite of software products and services that are seamlessly integrated into users' digital worlds, with over-the-air (OTA) updates that will add value over time"[218].

294. The conglomerate nature of hyperscalers also seems likely to generate network effects linked to data collection. These players have multiple sources of data collection at their disposal, enabling them in turn to increase the precision and attractiveness of the services they can propose in their cloud offerings. Data collected on other activities can be a lever for converting customers from other services to cloud services. In turn, the attractiveness of these cloud services will also help to boost their performance, and could therefore strengthen their position in their other businesses.

295. It therefore appears that several players enjoy significant conglomerate advantages that are difficult for pure players in the cloud sector to replicate. These advantages are likely to affect competitive dynamics. In particular, they can be used to generate leverage effects and therefore raise risks for competition (see Part IV).

E. COMPETITIVE DYNAMICS

296. An analysis of the cloud sector shows that its characteristics - from economies of scale and scope to preference for the most comprehensive offerings, ecosystem-based competition and conglomerate advantages - favour large incumbents, particularly when they provide diversified digital services. Market concentration can therefore be expected to continue, to the benefit of hyperscaler ecosystems.

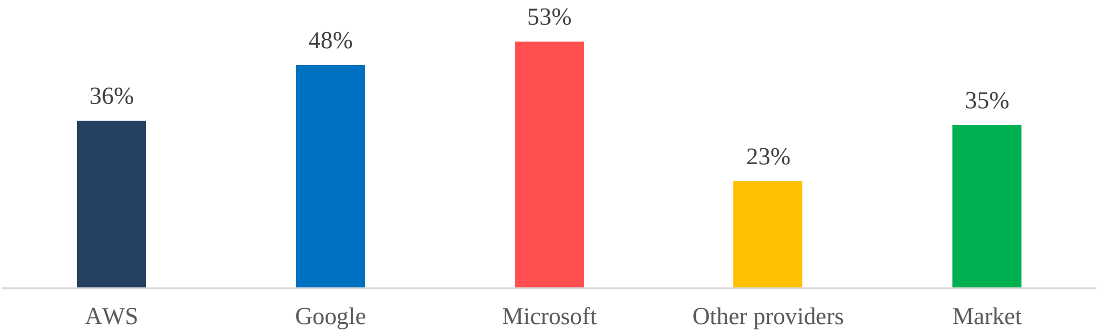
297. For the time being, the investigation shows that all the providers in the French market are experiencing strong growth in their business, due to the increase in demand for cloud services. Several players have also managed to grow and gain market share despite a later launch, such as Oracle Cloud, an infrastructure launched in 2016.

298. Within this trend, however, the ecosystems of the American hyperscalers - AWS, Microsoft and Google Cloud - are managing to experience most of this growth, and increase their market share as a result. According to a Markess study, AWS, Microsoft and Google Cloud captured 80% of the growth in spending on public cloud infrastructures and applications (IaaS and PaaS) in France in 2021[219]. Microsoft recorded the highest growth rate (see Figure 16).

[218] Press release of 5 January 2022, "Amazon and Stellantis collaborate to integrate connected customer-focused experiences into millions of vehicles, accelerating Stellantis' software transformation" (link).

[219] Le Figaro, "AWS, Microsoft and Google prevail in the cloud market in France", 19 May 2022 (link).

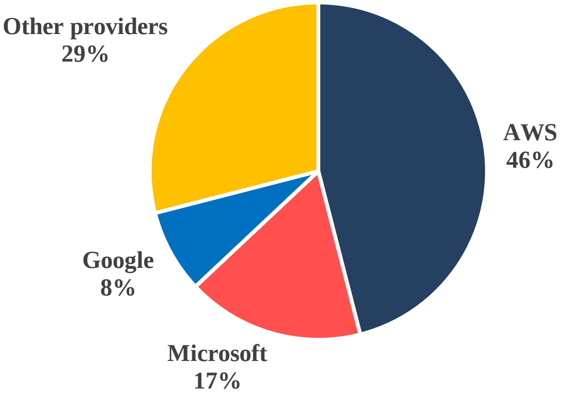
Figure 16 - Growth of IaaS/PaaS providers in France in 2021



Source: Markess by Exaegis.

299. This dynamic could strengthen the position of these large ecosystems, which already account for a significant percentage of revenues from IaaS and PaaS activities. The different definitions of cloud services, including the distinction between IaaS and PaaS services depending on the provider, make it difficult to collect data and accurately estimate market share. However, the various sources analysed by the *Autorité* tend to show that AWS and Microsoft are the two main providers of IaaS and PaaS services in France. According to Markess (see Figure 17), by 2021, AWS had captured almost half of IaaS and PaaS revenues in France (46%), with Microsoft's share amounting to around 17%.

Figure 17 - Percentage of IaaS and PaaS revenues in France in 2021 by provider



Source: Markess by Exaegis.

300. At European level, the trend is also towards faster growth for the largest ecosystems, which account for the majority of revenue growth in the cloud sector. According to data from Synergy Research Group, the European cloud market in September 2022 (including IaaS, PaaS and Hosted Private Cloud) was "*more than five times larger than it was at the start of 2017, reaching 10.4 billion euros in Q2 2022. Over the same period, European cloud providers increased their cloud-based revenues by 167%, but their market share fell from*

27% to 13% as their growth rate remained well below the overall growth of the cloud sector"[220]. This observation is confirmed by recent studies by ACM[221] and OFCOM[222].

301. The growth of the main providers cannot be explained solely by improved price competitiveness. According to an internal study by one hyperscaler, its prices were twice those of OVHcloud for the purchase of virtual machine instances in the public cloud in 2020. One cloud service provider also claimed to offer services up to 60% cheaper than AWS. However, according to this provider, this price competitiveness does not make it any more competitive in absolute terms, as price is not the only or even the primary criterion for choice.

302. These elements tend to confirm that the characteristics identified above play a decisive role in the competitive dynamic, and within it, in the privileged position of large ecosystems. In this context, the likelihood of a new operator being able to gain market share rapidly appears limited, except from operators who are already powerful in other markets. This probability could further decrease as the number of companies that have completed their migration and chosen a cloud ecosystem increases.

303. Lastly, the investigation revealed that the relative growth of hyperscalers is raising concerns, particularly in terms of dependence on a few providers. In the financial sector, for example, the BIS is alarmed at the increased dependence of banking institutions on major US providers, which could lead to systemic vulnerabilities[223]. This trend could affect a large number of sectors. In fact, according to AWS, over 80% of CAC 40 companies and over 70% of French unicorns[224] use AWS cloud services[225].

304. Given the risks of lock-in, the competitive pressure exerted by other providers could also become insufficient. ACM's market research also confirms that at least two of the leading cloud service providers generate significant margin rates from their cloud activities, with these profits making a very large contribution to their overall profits[226]. These findings call for particular vigilance with regard to changes in the market's competitive structure and to the practices likely to be implemented by cloud service providers.

[220] Synergy Research Group, "*European Cloud Providers Continue to Grow but Still Lose Market Share*", 27 September 2022 (link).

[221] ACM stated that "*Based on the revenue information obtained, ACM concludes that Azure, with a market share of between 40% and 45%, has the biggest market share in the Netherlands. AWS follows Azure with a market share of between 30% and 35%. After AWS and Azure, GCP and Oracle have the biggest market share, at between 5% and 10%. The "others" category contains cloud providers that only have a market share of a few percent. This includes operators such as Leaseweb and ODC-Noord*" (ACM market study, page 34).

[222] According to OFCOM, "*Market shares have remained concentrated towards the market leaders in recent years While Google is often positioned as the closest challenger and has been gaining share, it remains far behind in terms of size and is yet to make a profit. The other smaller cloud providers remain further behind*" (OFCOM interim report, page 190).

[223] Les Echos, "Cloud: alert on the dependency of banks on the web giants", 21 July 2022 (link).

[224] In economics, a "unicorn" is an unlisted company in the new technologies sector with a valuation of at least one billion dollars (link).

[225] AWS website, "Amazon Web Services invests in France for the long term", 27 September 2022 (link).

[226] ACM market study on cloud services, p. 63 (link): "*at least two major cloud providers are generating high profit margins, so profits from cloud services make up a very considerable share (30% to 40%) of the total profits of these big tech undertakings*".

How the cloud sector works

The *Autorité* notes that US operators such as Amazon, Microsoft and Google, that already have a strong presence in other sectors of the digital economy, benefit from significant competitive advantages over their French and European rivals. These *hyperscalers* enjoy considerable financial power, enabling them in particular to make the substantial investments that are nonetheless needed to launch activities in the cloud industry, such as in data centres or IT infrastructures. They can benefit from economies of scale and product ranges linked to their different activities. Finally, they have access to a 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.

Furthermore, although all cloud service providers operating in the French market are experiencing strong business growth, the major US hyperscaler ecosystems are benefiting from most of this growth. These operators have thus increased their market share. The three above-mentioned companies had captured 80% of the growth in spending on public cloud infrastructures and applications in France by 2021. The main dynamic in the French market over the next few years could therefore be the continuation of market concentration, to the benefit of the hyperscalers' ecosystems.

The different definitions of cloud services, including the distinction between IaaS and PaaS services depending on the provider, make it difficult to collect data and accurately estimate market share. However, the various sources analysed by the *Autorité* tend to show that AWS and Microsoft are the two main providers of IaaS and PaaS services in France. By 2021, AWS had captured almost half of IaaS and PaaS revenues in France (46%), with Microsoft taking around 17%.

The likelihood of a new operator being able to gain market share rapidly appears limited if it is not already powerful in other markets. This probability could further decrease as the number of companies that have completed their migration and chosen an ecosystem increases. Indeed, large hyperscalers organised into ecosystems enjoy competitive advantages over providers offering more limited catalogues of services, and competitive bidding will generally lead to the selection of a provider who will cover the customer's entire need, which is more like competiting *for* the market than *in* the market.

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

III. Analysis of relevant markets in the cloud industry

305. Defining the relevant markets is the first step in the competitive analysis of trade practices or proposed mergers, whether at national or European level. As the Commission points out in its proposal to revise its Notice on the definition of the relevant market for the purposes of EU competition law[227], published in November 2022 (hereinafter "*the draft Notice"), "in accordance with the case law of the Court of Justice or the General Court of the European Union and the Commission's decision-making practice, the relevant market within which the Commission assesses competitive dynamics is generally defined in terms of a product and a geographic dimension*".

306. The definition of a relevant market, in terms of both products and geographic dimension, must therefore make it possible to determine whether there are actual or potential competitors capable of influencing the behaviour of the companies present. Its fundamental objective remains the assessment of the market power of the different players involved, as part of the examination of potential anticompetitive practices and merger control.

307. The analysis in this opinion is therefore not intended to provide a detailed outline of the relevant markets in the cloud sector or to establish any links that may exist between these markets.

308. As the cloud sector is relatively new and still evolving, decision-making practice in this area is still limited. Indeed, at both national and European level, decisions involving elements of the cloud sector are mainly clearance decisions without merger control conditions and not litigation decisions[228]. These decisions have a forward-looking dimension and do not required a precise market definition.

309. In addition, the cloud sector is characterised by the coexistence, on the one hand, of a considerable heterogeneity of services, ranging from basic storage services to a specific service for a customer wishing to comply with regulatory obligations, and on the other hand, of offers that are part of digital ecosystems and grouped offers, which can make the delineation of the relevant market difficult.

310. The public consultation published on 13 July 2022[229], and the responses received during the course of the investigation, made it possible to gather the information available on the markets in order to specify the various quantitative and qualitative factors that are important from the point of view of demand and supply, and to identify the cloud products and/or services that could potentially form part of the same market. It should be noted, however, that the *Autorité* is relying on data collected as part of the investigation for this opinion, which was carried out between January 2022 and April 2023. As the cloud sector is

[227] The Commission Notice on the definition of relevant market for the purposes of Community competition law (OJ C 372, 9.12.1997, p. 5-13), published in 1997, is still in force. The revised notice was submitted for public consultation on 8 November 2022. A new Notice is due to be adopted in the third quarter of 2023.

[228] See, for example, Autorité de la concurrence Decision 19-DCC-259 of 18 December 2019 regarding the acquisition of sole control of Softeam by La Poste Group; European Commission Decision in Case M. 9205, IBM/Red Hat, 27 June 2019; European Commission Decision in Case M. 8994, Microsoft/Github, 19 October 2018; European Commission Decision in Case M. 6921, IBM ITALIA/UBIS.

[229] https://www.autoritedelaconcurrence.fr/en/article/autorite-opens-public-consultation-part-its-cloud-sector-inquiry.

particularly dynamic, the developments in this opinion are not intended to be set in stone, but to propose a method of analysis and points to reflect upon .

311. Firstly, the *Autorité* proposes a market analysis grid (A), dealing with demand substitutability (1) and then supply substitutability (2), which will then allow consideration of market segmentations in the cloud sector (B).

A. ANALYSIS GRID OF RELEVANT MARKETS IN THE CLOUD INDUSTRY

1. ANALYSIS OF DEMAND-SIDE SUBSTITUTABILITY

a) Analysis framework

312. According to the above-mentioned Commission Notice, "*A relevant product market comprises all those products and/or services which are regarded as interchangeable or substitutable by the consumer, by reason of the products' characteristics, their prices and their intended use, taking into account the conditions of competition and the structure of demand and supply on the market*" [230]. In particular, the draft Notice proposes taking into account the particularities of the digital environment when analysing the definition of relevant markets.

313. Therefore, in this case, different cloud products or services will be considered as competing when the ability of customers to compare them (even when prices, innovation or product quality differ) is such that they can be considered sufficiently interchangeable and belonging to the same product or service market. In its recent Google Android ruling, the General Court of the European Union pointed out that "*interchangeability or substitutability is not assessed solely in relation to the objective characteristics of the products or services at issue. The conditions of competition and the structure of supply and demand on that market must also be taken into consideration [see judgment of 30 January 2020, Generics (UK) and Others, C 307/18, EU:C:2020:52, paragraph 129 and the case law cited]*" [231].

314. In practice, this demonstration of demand-side substitutability involves, in this case, firstly identifying the smallest groups of candidate cloud products or services in the relevant markets, in other words, identifying the closest groups of substitutes. The second question is whether companies operating in these smaller markets would be able to raise their prices, or more generally downgrade their offerings, in a sustainable, significant and profitable way, or whether this downgrading leads to a sufficient proportion of demand switching to other cloud products or services.[232]

[230] Commission Notice on the definition of relevant market for the purposes of Union competition law, point 20 (link). See also the Decree of 30 January 2020, Generics (UK) and others, C-307/18, EU:C:2020:52, paragraph 129; and the Decree of 13 February 1979, Hoffmann-La Roche v. Commission, C-85/76, EU:C:1979:36, paragraph 51. Also, see the European Commission Staff Working Document on the Evaluation of the Notice on the definition of relevant market, published on 12 July 2021, which takes into account the new challenges posed by the digital sector (link). See also European Commission - Communication from the Commission 2018/C 159/01, Guidelines on market analysis and the assessment of significant market power under the EU regulatory framework for electronic communications networks and services.

[231] Judgment of the General Court of the European Union of 14 September 2022, Google Android, T-604/18, paragraph 106 (link to judgment and link to press release).

[232] Further details are available in the public consultation document published on 13 July 2022.

b) A demand likely to be formulated by workload

315. Competition authorities have already faced the challenge of defining new relevant markets in innovative sectors such as telecommunications and IT services. Like the cloud today, these sectors have seen strong growth and the rapid advent of new functionalities in a relatively short period of time. However, it has been possible to identify criteria for analysing the boundaries of the new relevant markets, taking into account in particular customer needs.

316. For example, in an article published in 1992, one author suggested that markets in the telecommunications sector could usefully be defined according to "functionality criteria". According to this author, services that meet the same needs from the consumer's point of view should be grouped together in the same market[233]. In addition, in the 1999 AT&T/IBM Global Network merger decision, the Commission analysed whether, after the merger, AT&T would have been in a position to restrict the provision of certain telecoms services to its competitors, namely service levels 1 (basic services such as local or long-distance leased lines) and 2 (addition of end-to-end service levels, such as router interconnection layers)[234]. At the time, the added value of telecoms services was identified as an additional criterion for defining relevant markets.

317. In this case, and without going so far as to consider that each functionality (or added value) would define a relevant market, a large proportion of the players interviewed or who responded to the public consultation indicated that they formulated their demand to providers by workload[235], which consume IaaS and/or PaaS services depending on their architecture. In most cases, workloads group together several categories of cloud services, as presented in the public consultation document published by the *Autorité* in July 2022. In this regard, a hyperscaler argued that: "*the workloads cited in paragraph 52 of the public consultation* [published as part of this opinion] *illustrate how cloud services can meet customers' needs. However, customer needs are constantly evolving and the services chosen to meet them can vary from one customer to another*."

318. Even when a workload has been identified, there are multiple ways of meeting it, with varying degrees of added value provided by the cloud operator. Some operators will offer a cloud service that meets part of a customer's expressed need, while others will be able to offer cloud services that could anticipate future customer demand, including new functionalities, such as moving from an IaaS service to a PaaS service. In this case, a separate market can probably only be identified once the new demand has taken concrete form. Other operators will have no difficulty in refocusing their production to meet a specific customer workload. The information collected during the investigation showed that the more customers look for integrated services, the more they will turn to providers able to cover all their needs.

319. One large corporate customer of cloud services reported that its public cloud (IaaS and PaaS) call for tender resulted in the selection of two providers following a dialogue involving several candidates based around three themes, including "*business needs (use cases, reversibility, architecture, cost monitoring, etc.)*".

[233] Matthias-Wolfang Stoetzer, "Value-added services - problems of definition and data", *Telecommuncations Policy*, July 1992.

[234] Case IV/M.1396, AT&T/IBM GN, 22 April 1999.

[235] On the definition of a workload, see above.

320. In this way, workloads can be substitutable when they meet the same customer needs. While there are offers with different degrees of added value for the same workload, the question arises as to whether they belong to the same relevant market. However, only a case by case analysis can determine the boundaries between these different workloads.

2. Analysis of supply-side substitutability

321. This analysis of demand-side substitutability can be complemented by an analysis of supply-side substitutability.

a) Analysis framework

322. The analysis of supply-side substitutability involves assessing whether most providers of cloud products or services would be "*in a position to switch production from one product to another in the related product range, while bearing only negligible additional risks or sunk costs, whether they have an incentive to do so when relative prices or relative demand conditions change, and whether, moreover, they can effectively market these other products in the short term*" [236]. According to the above-mentioned Commission Notice, "*situations of sufficiently strong supply substitutability can generally arise when companies market different qualities or categories of the same product*" [237]. For example, in the Oracle/Sun Microsystems case, the Commission considered delineating the relevant database market by taking into account supply-side substitutability, which would have made it possible to include all database products in a single market[238].

323. Thus, for a given workload (which includes all the services associated with that workload), it is essential to determine whether providers can redirect their production to that workload without substantial additional costs, and within a short timeframe. With regard to custom-made products[239], the Commission states that "*when the same providers are able to react, and generally do react, by submitting offers that meet the requirements of different customers, custom-made products can be included in the same relevant product market*"[240]. One hyperscaler argued "[that] *it is also possible for the same customer to use several separate cloud providers for the same workload, with this workload being managed by different services offered by different cloud providers*." However, while using multiple cloud service providers for a single workload might be theoretically possible, it remains rare and expensive for a company to do so[241].

[236] Commission Notice on the definition of relevant market for the purposes of Union competition law, point 35 (link).

[237] Commission Notice on the definition of relevant market for the purposes of Union competition law, point 36 (link).

[238] Case COMP/M.5529, Oracle/Sun Microsystems, 21 January 2010, paragraph 87.

[239] In the case of custom-made products, pre-existing products are put together. However, the same reasoning could apply to cloud services.

[240] Commission Notice on the definition of relevant market for the purposes of Union competition law, point 37 (link).

[241] In any case, no examples were brought to the Autorité's attention during the investigation of this opinion. However, some customers may be tempted to use multiple cloud service providers for a single workload if they subscribe to different services via the marketplace on the main provider's website (see developments on marketplaces above).

324. Ever since cloud services have been on the rise, new products have been appearing on a regular basis, which seems to demonstrate that providers are capable of rapidly reorienting their development capacities to meet new needs.

325. The following example illustrates this type of service development reorientation by a cloud service provider. One IaaS service provider offers virtual machines, online storage and network services to its customers. This provider decided to reorient its cloud services production towards PaaS services. As part of this reorientation, it is developing a cloud platform that offers a complete development and runtime environment for applications. Customers will be able to develop, deploy and manage their applications on this new platform, without having to worry about the underlying infrastructure. To achieve this service reorientation, the provider will need to make several changes, such as investing in the development of new features and services for the PaaS platform, and training its in-house team so they acquire the skills needed to design, develop and maintain the new platform. This IaaS service provider, now also present in PaaS, will then be in a better position to offer an integrated solution that is better adapted to the workload formulated by the customer.

326. The development of PaaS services is facilitated by the ability to leverage existing infrastructures (IaaS). Furthermore, some of the necessary skills could also be pooled. This point was confirmed by one hyperscaler, who considered that a player can develop "*its own services or new services based on existing products. For example, a provider who already offers IaaS would be able to develop PaaS solutions relatively quickly, given the complementary nature of the products*". As a result, IaaS service providers have a number of advantages for expanding into PaaS and providing competitive integrated services. While this analysis tends towards a definition of markets that *a priori* includes only cloud service providers offering a larger quantity of services, only a case by case analysis will make it possible to define the exact outlines of the relevant markets.

327. Analysing supply-side substitutability therefore makes it possible to identify more substitutable products. Furthermore, even if there were no supply-side substitutability, the *Autorité* could nevertheless take into account the competitive constraints exerted by providers who would be able to redirect their production, without, however, strictly fulfilling the criteria for analysing the relevant markets.

b) Market definition in the presence of "digital ecosystems"

Consideration of cloud and non-cloud ecosystems

328. The analysis of relevant markets can also take into account cloud ecosystems (i.e. including cloud services present in different categories of the sector, including marketplaces (see Part II)[242]) or non-cloud ecosystems (i.e. including products or services related to the cloud, but which would prove necessary or useful for launching a cloud offer). The General Court of the European Union, in the aforementioned Google Android judgment, recently emphasised that "*[i]n a digital 'ecosystem', which brings together several categories of provider, customer and consumer and causes them to interact within a platform, the products or services which form part of the relevant markets that make up that ecosystem may overlap*

[242] As a reminder, an analysis of the way the sector operates, and the positioning of the different players, tends to show that some are building cloud ecosystems, i.e. a set of integrated services that customers can access, including the provider's proprietary services, but also, generally through available marketplaces, a set of services from third-party developers, designed to operate within this ecosystem.

or be connected to each other on the basis of their horizontal or vertical complementarity[243]. *Taken together, the relevant markets may also have a global dimension in the light of the system that brings its components together and of any competitive constraints within that system or from other systems*"[244].

329. The aforementioned draft Notice states that "[d]*igital ecosystems can in certain circumstances be considered as consisting of a primary commodity and several secondary (digital) products whose consumption is connected to the primary commodity, for example through technological links or interoperability. When examining digital ecosystems, the Commission can therefore apply principles similar to those applied to after-sales markets to define the relevant product market(s). Where secondary (digital) products are offered in a bundle, the Commission may also assess whether this bundle alone constitutes a relevant market. Although not all digital ecosystems correspond to an after-sales or bundled market approach, the Commission may, in any event, take into account elements such as network effects, switching costs and single and/or multihoming decisions for the purposes of defining the relevant product market(s)*" [245]. The authors of the Commission's final report on competition policy in the digital age had already envisaged such a market definition in 2019: "*Where the firms' lock-in strategies are successful, and consumers find it difficult to leave a digital ecosystem, ecosystem-specific aftermarkets may need to be defined*" [246].

330. However, information collected during the investigation showed that bundled offers may exist, particularly from providers organised into ecosystems. For example, one PaaS service provider argued that "*the level of granularity proposed* [in the public consultation document] *seems excessively fine to us, whereas the reality of the market is the confusion of most of the service categories listed within the same cloud provider platforms, with customers expecting to find most of these categories in a unified or at least centralised offering*". In addition, a number of services are interconnected or need to be used together to function properly (see Part II.C.1).

331. This means that cloud service providers who can directly meet a demand for bundled offers, or can potentially meet future customer needs for value-added services without making heavy investments, could possibly be considered competitors in the same relevant market.

332. It is clear from the above that it is very difficult to clearly define a workload *in abstracto*. Some customers will have a specific demand for a particular service, such as a database. The offer of this specific service will involve all the providers of this specific service. Other customers will have workload demands that require more cloud services in different categories (IaaS and PaaS services, for example). In this case, only providers who can meet the entire workload can be considered competitors. When analysing relevant markets in the cloud sector, it is therefore necessary to take into account not only demand-side substitutability but also the structure of supply, in order to identify competitors and their market power.

333. Moreover, in the case of cloud ecosystems, two cases could be considered:

[243] See related market developments below.

[244] Judgment of the General Court of the European Union of 14 September 2022, Google Android, T-604/18, paragraphs 116 and 129 (link to judgment and link to press release).

[245]Commission Notice on the definition of relevant market for the purposes of Union competition law, point 103 (link).

[246] Report by Jacques Cremer, Yves-Alexandre de Montjoye and Heike Schweitzer for the European Commission, Competition Policy for the digital era, Final report 2019, page 4 (link). Paraphrased.

- either the services offered by a cloud service provider are linked by interoperability, network effects or even switching costs, meaning that the ecosystem could constitute a single relevant market. This could be the case, for example, when a customer wants to migrate a workload already in the cloud to another cloud service provider;
- or the services offered by cloud service providers could each meet a workload, in which case the cloud service providers structured in ecosystems could be considered competitors in a single relevant market. This could be the case, for example, when a customer wants to make the first purchase of the cloud services that are needed to migrate a workload which requires cloud services in several IaaS/PaaS or even SaaS categories.

3. Reminder and analysis of possible approaches put forward in the public consultation

334. In the public consultation, the Investigation Services considered several possible relevant markets, ranging from the narrowest to the broadest, from the type of cloud service to the entire IT services market.

335. Firstly, it was proposed that a market be defined by type of cloud service, corresponding for example to document data storage or a relational database management system. Secondly, it was proposed that markets be defined by category of cloud services, which would group together several types of cloud services. Examples cited included data analysis, computation, containers, databases, developer tools, the Internet of Things, artificial intelligence and machine learning.

336. In their responses to this consultation, some corporate cloud service customers indicated that there would be a degree of substitutability between cloud service types, even if the use of these service types was not equivalent. The same would be true for categories of cloud services, which are sometimes grouped together in service packages offered by providers. However, as the responses to the public consultation were very disparate, it was not possible at this stage for the *Autorité* to more precisely consider the relevant markets by type or category of cloud service. This is without prejudice to the possibility that the *Autorité* may adopt a more refined definition of markets, corresponding to a type or category of cloud service, in the future, as part of a case by case analysis of a practice or proposed merger.

337. Segmentation based on IaaS/PaaS models was also envisaged. As mentioned earlier (see Part I), using these categorisations enables customers to focus the discussion on their cloud service needs. There are different levels of responsibility between providers and customers in the IaaS and PaaS segments. However, such segmentation does not necessarily seem relevant, as the boundaries between IaaS and PaaS are not clearly demarcated.

338. Lastly, some players, such as Amazon, had even proposed defining a cloud services market as a segment of a more global IT services market. However, the information collected during the investigation for this opinion seems to show that there is a specific demand for services operated outside the company’s premises. The vast majority of respondents indicated that they want or have wanted to migrate services to the cloud for reasons of flexibility and adaptation to their needs, which is not possible on-premise. On the other hand, some companies are choosing to migrate only part of their workloads to the cloud and keep other services such as software on-premise, which would show that these two deployment modes are offered in complementary rather than substitutable markets.

B. APPLYING THE ANALYSIS GRID TO THE CLOUD SECTOR

339. The *Autorité* will first propose a delimitation of products and services in the cloud sector (1), before analysing the geographical scope of the markets envisaged (2).

1. PRODUCT AND SERVICE MARKETS

340. Based on the analysis grid described above, the *Autorité* has drawn up a number of proposals for the possible delimitation of relevant markets in the cloud sector (as a reminder, the opinion analyses the operation of competition on the IaaS and PaaS layers, to the exclusion of the SaaS layer). These proposals are not exhaustive and are determined on the basis of the information collected during the investigation, over a limited period. Markets in this sector are exclusive to other IT markets. The *Autorité* then considers other related markets.

a) Proposed market definitions for the cloud sector

341. The *Autorité* suggests other possible market segmentations, on the one hand by SecNumCloud-certified workloads, and on the other by sectors subject to specific regulations.

"SecNumCloud" offers likely to be subject to specific segmentation

342. The investigation confirmed that customers can either use traditional public cloud offerings to meet their workload needs or use service offerings based on more stringent data protection requirements. Segmentation based on the SecNumCloud security authorisation (or trusted cloud, as ANSSI does not seem to distinguish between the two designations[247]) could therefore be justified if certain criteria were met.

Use of the SecNumCloud standard as part of the French government's "cloud at the centre" policy

343. From the point of view of the analysis of relevant markets, competition authorities examine whether the existence of a legal standard or specific regulation is likely to influence demand behaviour, insofar as it may influence the price of products, their quality or the perception that consumers have of them.

344. As indicated above (see Part I), since May 2021 the "cloud at the centre" doctrine has called for the cloud to become the default hosting method for all State digital services[248]. In this context, circular 6282-SG of 5 July 2021[249] therefore provides that the digital services of

[247] According to ANSSI, "*the SecNumCloud security authorisation is based on a demanding set of standards* [...]. *It identifies "trusted" cloud service offerings, i.e. those demonstrating a high level of skill and quality of service in cybersecurity, while at the same time offering strong protection for sensitive data*" (link).

[248] https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud/.

[249] Circular 6282-SG specifies that "*if the IT system or application handles particularly sensitive data, such as the personal data of French citizens, economic data relating to French companies, or business applications relating to government employees, the commercial offer selected must comply with SecNumCloud qualification*

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.

345. The SecNumCloud reference framework developed by ANSSI therefore constrains demand from public-sector players, insofar as the French government allows its departments and the organisations under its supervision to use these services under certain conditions. The government wants to go even further, by encouraging OVIs, OESs and local and regional public authorities to use the cloud and SecNumCloud offers for sensitive data[250]. Interviews conducted by the *Autorité* also revealed that a number of private and public sector companies, concerned about protecting their sensitive data, are interested in the prospect of being able to use offers that meet the criteria of the trusted cloud:

- 87% of respondents to the questionnaire sent out by the *Autorité* to customers in the cloud sector believe they hold sensitive data as defined by the Government as part of the national cloud strategy[251]. One of them stated that it was "*waiting for trusted managed services and offerings to extend the scope* [of its public cloud] *to sensitive data*";
- Cigref, which brings together some 150 major French companies and public administrations, all users of information systems, has confirmed that the trusted cloud meets a real need among its members: "*the need for a trusted cloud with an extensive catalogue of services has been clearly expressed by Cigref members, to guarantee the security of their sensitive data and associated processing, clarify the legal regime to which they are subject, protect them from non-European legislation, and control their dependency on their providers*" [252]. The association has also published a number of reference documents to promote the emergence of a "trusted cloud" doctrine and harmonise the needs of companies and public administrations, with the aim of inspiring the various initiatives in this field at both national and European levels[253];
- Cigref members welcomed the announcement of the national cloud strategy, as confirmed by the CEO of TotalEnergies: "[i]*n a context marked by the emergence of cybercrime and the rise of extraterritorial regulations, Total welcomes the publication of the French government's trusted cloud strategy with great interest. It will promote the emergence of service offerings that meet the technical and legal protection needs for its data, and enable it to benefit confidently from the digital revolution to support the energy transition*" [254].

(or a European qualification of at least equivalent level), and be immune to all extra-Community regulations," pages 10-11.

[250] Press kit, National Cloud Strategy: supporting innovation in the cloud", 2 November 2021, page 26.

[251] As part of its National Cloud Strategy, the French government has defined sensitive data as including the personal data of French citizens, economic data relating to French companies, and business applications relating to government employees.

[252] https://www.cigref.fr/la-strategie-nationale-pour-le-cloud-un-grand-pas-vers-la-maitrise-de-notre-destin-numerique.

[253] https://www.cigref.fr/le-cigref-publie-son-referentiel-du-cloud-de-confiance.

[254] https://www.cigref.fr/la-strategie-nationale-pour-le-cloud-un-grand-pas-vers-la-maitrise-de-notre-destin-numerique.

346. This new doctrine is beginning to have an impact on the market. One hyperscaler confirmed that it has received several requests to halt projects from government ministries and public bodies, as they await future SecNumCloud offerings to meet their needs.

Some customers are looking for a high level of data security, and above all immunity against extra-European laws, which they do not feel is guaranteed by non-SecNumCloud-certified offerings

347. Today, most customers host their sensitive data in the cloud. According to the Cloud Security Alliance, an association tasked with promoting security best practice in the cloud, 89% of the entities surveyed host their sensitive data or workloads in the cloud, with 67% in the public cloud and 45% in the private cloud[255] (a company can potentially host sensitive data in both the public and private clouds). The *Autorité's* investigation has also shown that, for some companies, the public cloud is an effective deployment model, offering guarantees that they consider sufficient in terms of security, particularly encryption.

348. For other companies, however, existing public cloud offerings could not be substituted with "trusted cloud" offerings from a demand perspective. The investigation showed that SecNumCloud certification was attractive, particularly in view of extraterritorial legislation deemed highly intrusive on data stored and processed in the cloud. Several respondents to the *Autorité's* public consultation and online survey confirmed that "trusted cloud" offers would enable them to position new workloads in the public cloud:

- one customer pointed out that data security and sovereignty protection are not currently sufficiently guaranteed by hyperscalers' offerings. The emergence of new SecNumCloud offerings will potentially enable it to place new workloads on a public cloud;
- another customer stated that its current strategy is to minimise the amount of data that needs to be transferred to the public cloud and avoid entrusting it with sensitive data. Eventually, 40% of its applications could be outsourced to trusted cloud service providers, and around 20% to traditional public cloud service providers.

349. These characteristics should be taken into account to determine whether SecNumCloud offers can be distinguished from other non-certified offers.

Higher prices

350. Cloud service providers seem to be anticipating higher prices for "trusted cloud" solutions, in the order of 20% according to some press reports[256]. Some industry players pointed out that the SecNumCloud standard would justify revising the existing architecture, training staff in this technology and devoting a specific annual budget to maintaining the integrity of the existing system.

351. If such a price differential were to be established, it would also have to be taken into account when assessing any market segmentation.

[255] Cloud Security Alliance, Sensitive data in the cloud, 7 December 2022 (link).

[256] https://www.forbes.fr/technologie/systemes-dinformation-faut-il-tout-miser-sur-le-cloud-de-confiance/.

Supply-side substitutability

352. Setting up a SecNumCloud-certified offering requires considerable legal adjustments and investment on the part of cloud service providers.

353. As previously mentioned (see SecNumCloud box), the SecNumCloud 3.2 standard issued by ANSSI now includes provisions for protection against non-European law. This protection is based in particular on the assurance that the cloud infrastructure will be used by a company subject exclusively to the laws of the European Union, and on the compartmentalisation of the SecNumCloud-certified IT environment. Updating the standard therefore required significant legal adaptations for hyperscalers, who had to create new structures entirely controlled by third parties. These hyperscalers will also need to set up a separate public cloud infrastructure with local control, which will entail upgrade and maintenance costs.

354. Even if some smaller cloud service providers do in fact meet some of the requirements of the standard, particularly in view of their nationality, the fact remains that SecNumCloud certification requires substantial technical investment to meet the necessary security requirements. Some cloud service providers indicated that they do not want to apply for ANSSI certification so that they can devote more time to developing their business in the sector, particularly through innovation.

355. A possible segmentation based on SecNumCloud offers could therefore be envisaged, subject to a practical assessment of all the above elements. Other certifications could be subject to comparable reasoning in the future.

Segmentation by sector is not an option today

356. Segmenting the market according to the sector concerned on the demand side could be justified if customers considered that the cloud products and/or services they needed could not be substituted with the cloud products and/or services offered to other sectors[257].

357. Certain sectors are therefore subject to a high level of technological and regulatory requirements.

358. For example, the French Public Health Code (*Code de la santé publique*) (Article L. 1111-8) requires service providers hosting certain types of protected health data to obtain HDS certification (see Part I.B.c.). The question of segmentation between HDS-certified and non-HDS-certified providers could therefore arise.

359. HDS certification provides a framework for strengthening the security of protected health data. To obtain HDS certification, providers must comply with a detailed list of requirements for activities involving the provision of physical hosting premises and hardware infrastructure and/or activities involving the provision of virtual infrastructure and software platforms, as well as administration/operation and outsourced backup[258]. They must also be ISO 27 0001 certified. However, the investigation revealed that all cloud service providers

[257] In a number of decisions concerning IT services, market segments have been created on the basis of customer activity. For example, the French competition authority considered the existence of a market for integrated management software packages for the liberal accounting professions when examining a merger (French competition authority, Opinion 05-A-24). In addition, the Commission had identified, but not definitively ruled on, a market for customer relationship management software based on the customer's sector of activity (Case COMP/M8274 Cinven/Permira/Allegro/Ceneo of 21 December 2016).

[258] https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante.

are HDS-certified hosters[259], but not necessarily for all the activities covered by this certification. For example, Scaleway is certified only for "*the provision and maintenance in operational condition of the hardware infrastructure of the information system used for processing health data*"[260].

360. The financial sector is also subject to stringent regulatory requirements, which may justify specific segmentation. In particular, they require the implementation of special contractual conditions, such as effective audit rights, as well as business continuity and reversibility plans. The DORA regulation strengthens the rules for managing the risks associated with new technologies in the financial sector, by introducing specific contractual clauses and a framework for supervising third-party service providers, including cloud service providers.

361. However, the investigations revealed that customers in regulated sectors do not appear to be looking for sector-specific cloud products or services in the catalogue of cloud service providers, as confirmed by a customer operating in the health sector. Its expectations are more focused on the ease with which it can switch providers and its ability to collect large volumes of data.

362. This finding was confirmed by cloud service providers, who indicated that they offer their cloud products or services to all their customers, regardless of the sector in which they operate. Customers can therefore decide to subscribe to specific products, developed for healthcare and life sciences companies for example, or to services combined by the customer as "*building blocks*" designed to meet specific professional or technical needs. In the financial sector, one hyperscaler confirmed that "*if you are a bank and you need character recognition functionality on a cheque, for example, this function is integrated and offered as standard in the category of services that use AI. This application developed on the cloud will not be developed solely for this purpose, so to create a complete application, the company will have to adopt a "menu" approach to meet its customers' business needs*".

363. Segmentation according to sector does not therefore currently seem relevant. However, it cannot be ruled out that such segmentation may be possible in the future, depending on changes to regulatory requirements.

b) Possible related markets

364. As already mentioned (see Part I), there are other products and services within the cloud value chain that do not constitute cloud services *per se*, but interact with them, either upstream or downstream of the value chain. These products and services can then be subject of a separate market definition, but one related to the cloud services under consideration.

365. A related market is defined by decision-making practice as a market which is related to the relevant market(s) under consideration, and which must be taken into account when analysing the conglomerate effects of a merger or anticompetitive practice[261]. In particular,

[259] https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies.

[260] https://esante.gouv.fr/offres-services/hds/liste-des-herbergeurs-certifies (consulted on 6 April 2023).

[261] See in particular Autorité Decision 09-DCC-28 of 30 July 2009 regarding the acquisition of sole control of POWEO by Österreichische Elektrizitätswirtschafts - Aktiengesellschaft, paragraph 27. According to the Paris Court of Appeal (Cour d'appel de Paris) , two distinct markets are likely to have a close nexus (*translated) "either because they are upstream or downstream of each other, or because they concern similar services, if not completely substitutable"* (Decree of the First Chamber - Section H of 31 March 2009, 2008/11353, page 10).

it is interesting to note that, in the cloud sector, a number of products or services found in markets other than the cloud can be used as levers by certain players to win and consolidate a customer base in the cloud services markets (see Part IV).

366. In the present case, the *Autorité* examined three types of market related to those for the provision of cloud services: the market for colocation services in data centres (a), the software markets (b) and the intermediation markets for consulting and integration of cloud solutions (c). This does not rule out the possibility that other related markets may be identified when analysing cases that may arise in the cloud sector.

The market for data centre colocation services

367. European and national decision-making practice distinguishes the market for data centre colocation services from other IT services[262]. In this respect, the Commission recalls that data centres are dedicated facilities in which companies host and operate the IT equipment that supports their business (servers and data storage, for example). Data centre customers pay recurring fees for renting space in the data centre to install their IT equipment, as well as for using the building's energy. These types of service are generally called "colocation services", because several customers use the same data centre.

368. The Commission has excluded from the colocation services market "in-house data centres", i.e. those used exclusively for the needs of the company to which they belong, given the differences in price and characteristics between in-house data centres and colocation data centres[263]; the latter make it possible to pool and optimise the allocation of resources (servers and other physical components).

369. The information collected for this opinion leads to the same conclusions, namely that the colocation services offered by data centre operators and the services provided by cloud service providers do not appear to be substitutable. While some cloud service providers build their own data centres, these are used for their own purposes, i.e. to provide cloud services to their customers, not to lease locations to other cloud service providers.

370. The offerings of cloud service providers and data centre operators are therefore distinct, because they do not meet the same demand. One PaaS service provider, for example, stated the following with regard to the substitutability of the services offered by a data centre operator and a cloud service provider respectively: "*Substitution is not possible if the service the customer is looking for is a software solution designed to simplify its use of cloud infrastructures (e.g. renting servers in a data centre rack, which the customer has to configure and administer itself, cannot be substituted by a PaaS-type solution).*" However, the data centre colocation market could constitute a related market, as it would be upstream of the cloud services offered by cloud service providers.

[262] See Commission Decision COMP/M.7678 of 13 November 2015, Equinix/Telecity, notably contained in the Autorité's Decision 19-DCC-259 of 18 December 2019 regarding the acquisition of sole control of Softeam by La Poste Group, paragraphs 32 to 37.

[263] Commission Decision COMP/M.7678 of 13 November 2015, Equinix/Telecity, paragraph 16, contained in the Autorité's Decision 19-DCC-259 of 18 December 2019 regarding the acquisition of sole control of Softeam by La Poste Group, paragraph 35.

Software markets

371. The investigation showed that, as a result of their links with cloud services, software markets could be considered related markets that could be taken into account for competitive analysis in the cloud sector.

372. As previously mentioned (see Part II.C.1), the technology stack comprises the hardware layer (servers, data storage units and personal computers used directly by the company's employees) and the software layers (operating system, database, middleware and company software applications) [264].

373. In a 2012 decision, the *Autorité* stated that "*all the layers of the technology stack are essential to the operation of any company's IT system. Furthermore, only their interoperability allows them to work together*." The *Autorité* concluded that *"the indispensable nature of interoperability between the different components of a computer installation attests to the existence of a close link between the product markets linked to the different layers of the technology stack*" [265].

374. Before the development of cloud services, the software in the technology stack was installed on-premise, on customer companies' own servers, and distributed in the form of (perpetual or renewable) licences by software vendors. With the rise of the cloud, this software is also available on demand, in the form of cloud services. In this case, they are distributed as PaaS products (like certain Oracle database software), or, more often, SaaS (like the Microsoft 365 suite). Their deployment methods have therefore evolved within companies. In a merger decision, the Commission left open the question of a finer segmentation of the customer relationship management software market according to deployment method, more specifically between on-premise installation and hosting (SaaS mode)[266].

375. The connection between the software and cloud markets was also noted in a report published in October 2021 on behalf of CISPE (Cloud Infrastructure Services Providers in Europe). The report identified certain software products as "adjacent" to cloud services.[267] It emphasised that this software could be acquired via integrated PaaS or SaaS solutions, or separately and then integrated into an existing cloud infrastructure solution. However, some software is necessary for the provision of cloud services, and companies already historically present in the on-premise software sector would therefore have an advantage in providing this software in the cloud.

376. Software vendors such as Microsoft, IBM and Oracle are now major players in the cloud. As the different technology layers are characterised by strong interoperability links, making all these markets related to each other, a company in a dominant position in one of these

[264] Case COMP/M.5529, Oracle/Sun Microsystems, paragraphs 24 and 29. The Commission had also envisaged market segmentation according to the sectors of activity for which the software was intended, as well as according to the end-uses of the software (as part of the end-use segmentation, the Commission studied the high-end, mid-range and low-end software markets separately (Commission Decision COMP/M.6237 of 20 June 2011, Computer Sciences Corporation/iSoft Group, paragraph 22). See also Decision COMP/M.5763 of 29 March 2010, Dassault Systèmes/IBM DS PLM Software Business and COMP/M.5904 of 20 July 2010, SAP/Sybase).

[265] Decision 12-D-01 of 10 January 2012 regarding a request for interim measures concerning practices implemented by the companies Oracle Corporation and Oracle France, points 15 and 16.

[266] Case COMP/M.8274, CINVEN/PERMIRA/ALLEGRO/CENEO, 21 December 2016, paragraph 42.

[267] Frédéric Jenny, "*Cloud Infrastructure Services: an analysis of potentially anti-competitive practices*", October 2021, paragraph 23.

markets could use its market power to exclude its current or potential competitors from other markets, in particular cloud markets. Indeed, factors such as compatibility, interoperability and level of integration could have a major influence on customers' choice of cloud services.

377. It would therefore seem that these markets must 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, leverage effects could emerge in cloud markets due to the dominant position of certain software players also present in cloud markets; this would have the effect of excluding cloud service providers absent from these related markets (see Part IV).

The intermediation market for consulting and integration of cloud solutions

378. As mentioned above (see Part I), cloud service providers can either contract directly with their end customers or use a physical or virtual intermediary to sell their services. These intermediaries act as prescribers of cloud offerings. A number of intermediation markets have emerged in the digital sector in recent years[268]. However, intermediation markets in the cloud sector are interesting to analyse insofar as the companies present in these markets are also present in the cloud markets.

379. For the purposes of this opinion, the *Autorité* considered the existence of a market for consulting and integration of cloud solutions. This does not rule out the possibility that other intermediation markets in the cloud sector may exist or be envisaged.

380. When a customer wants to buy cloud services, they can do so directly from the provider, or through intermediaries. These intermediaries are IT professionals responsible for integrating several cloud services into customers' information systems. DSCs[269]s have the ability to advise their customers on which cloud solutions to consider, advise their providers on how best to satisfy customers, handle implementation services (including integration), customise and develop a solution tailored to a customer's particular needs, or operate as resellers of cloud solutions, with a view to eventually entering into partnership agreements with cloud service providers. These services are the same as those provided by consulting companies for corporate application software integration. This situation has already been studied by the Commission[270].

381. As such, these integrators do not provide cloud services directly to their customers, but - unlike cloud service providers - are able to offer a wide range of services from multiple providers. Some integrators define themselves as neutral when it comes to cloud service providers, highlighting their partnerships with all of Europe's leading cloud service providers. Furthermore, some customers who use a cloud service provider are at a very advanced stage in their thinking and already know which specific services they need, whereas integrators are involved further upstream in defining the needs of customers less familiar with cloud topics.

382. The investigation revealed that most requests for integration or consulting services from third parties are from large companies wanting to migrate some or all of their workloads to

[268] See, for example, Commission Decision AT.40411 of 20 March 2019, Google Search (AdSense), which distinguishes a market for intermediation services for the sale of online advertising, and the Autorité's Decision 21-D-11 of 7 June 2021 regarding practices implemented in the Internet advertising sector, which identifies the existence of a market for platforms selling online advertising space not linked to searches.

[269] See Part I.C for their presentation

[270] See Commission Decision COMP/M.3216 of 26 October 2004, Oracle/PeopleSoft, paragraphs 53 and 54.

the cloud. On the supply side, some cloud service providers offer these support and integration services (such as Microsoft), while others offer very few (such as AWS). However, it is always technically possible for a third party to integrate cloud solutions offered by a cloud service provider.

383. One cloud service provider sums it up this way: "*Most cloud providers do not really offer consulting and support services that are accessible to all their customers. Even training courses are generally offered by third parties (for example, the best-known AWS certification course is offered by Udemy). AWS currently tends to rely on third parties, whatever the size of the customer. For Microsoft, it is a different story. It has historically had a division dedicated to key accounts and therefore supporting them with their Cloud offerings. However, it is entirely possible for third parties to replace them. This is the advantage of APIs: the possible functionalities are perfectly described in their documentation. This will be a major growth driver for DSCs (who provide support), ISVs (independent software publishers, who produce tools) and managed service providers (who operate) in the years to come*."

384. However, if the cloud service provider offers support or the integration of cloud services to a customer wanting to migrate its workloads to the cloud, that provider, like Microsoft, will offer the integration of its own cloud solutions. Third-party companies, on the other hand, will either be neutral towards cloud service providers or will have entered into partnerships with certain cloud service providers to offer their solutions as a priority. In this way, integrators sometimes act as resellers or specifiers of cloud services without limiting themselves to a single cloud service provider, but could also be influenced by partnerships they have set up with certain cloud service providers. The *Autorité* will therefore remain vigilant in this respect, as this prescriptive role can be decisive in the market (see Part IV).

385. In view of the above, it might therefore be possible to consider defining a relevant market for the intermediation of consulting and integration of cloud solutions.

2. GEOGRAPHIC MARKETS IN THE CLOUD SECTOR

386. As the European Court of First Instance recalled in the recent Google Android case, "*In its geographical dimension, the relevant market is the territory within which the conditions of competition are the same and form an area which is sufficiently homogeneous to be considered in its entirety and to enable the effect of the economic power of the undertaking concerned to be evaluated (see, to this effect, the judgment of 14 February 1978, United Brands and United Brands Continentaal v. Commission, 27/76, EU:C:1978:22, points 11, 44, 52 and 53)*"[271]. The defined market can be distinguished from neighbouring geographical areas particularly because the competition conditions differ appreciably.

387. The information collected during the investigation points to the possibility of geographic markets whose boundaries would be determined by criteria of sovereignty, data use or latency, for example.

388. As a result, the markets envisaged above would not *a priori* all have the same geographical dimensions. For example, a workload that is not subject to SecNumCloud certification requirements could have a European or even global dimension, while a workload requiring

[271] Judgment of the General Court of the European Union of 14 September 2022, Google Android, T-604/18, paragraph 107 (link to judgment and link to press release).

a high degree of security (using military or banking data, for example) could be restricted to the national or European territory. Trusted cloud offerings are specific to France, and could lead to a more refined delimitation of the market pending European certification (see Part I). The need to comply with the GDPR could also justify a national or European delimitation of markets. One retail conglomerate pointed out that "*the choice is made in favour of cloud providers with infrastructures in Europe, mainly for reasons of personal data regulation and the minimisation of geopolitical risks*".

389. Language could also be a criterion for geographical distinction. For example, one public company considered that "*the relevant markets should be defined at national and European level. While technically, cloud technology should make it possible to operate remotely, thereby erasing all geographical barriers, in reality, for commercial success and to meet language requirements, human resources (sales and support) must be present in the target countries. The markets could therefore be considered national in scope*." This could be the case, for example, in the market for consulting and integration of cloud solutions, as envisaged above.

390. In addition, customers are looking for cloud service providers with a data centre in the geographical area of their own end customers, on a national or continental scale. It is the proximity of the data centre that determines the bidirectional latency corresponding to the ins and outs of an instruction (access to a programming interface, software control, data transfer). The geographical dimension may therefore depend on customers' technical and functional constraints, but also on network requirements.

Analysis of relevant markets in the cloud industry

The *Autorité* found 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 on a case by case basis. 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.

Segmentation based on SecNumCloud certification could also be envisaged. Indeed, the "cloud at the centre" doctrine, published 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.

The *Autorité* could therefore take into account all the circumstances of the case in point, such as the existence of functionalities differentiating them from non-certified offers, or a possible price differential, when assessing a possible market segmentation.

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, leverage effects could come into play in cloud markets, given the dominant position of certain software companies also present in the cloud.

IV. Competitive risks in the cloud industry

391. Given the way markets operate, their importance to the economy and the potential competitive advantages of certain players, it is vital that competition on the merits is fully expressed in the cloud sector. The *Autorité* has therefore analysed a number of practices implemented or likely to be implemented in this sector, which could restrict competition.

392. Several competitive risks have been identified on the basis of this analysis. Beyond the market failures that can be identified (see Part VI), certain risks raise cross-cutting issues, insofar as they affect competition in the sector as a whole (A). Others are more in line with specific scenarios (B), with risks identified when first migrating to the cloud and when migrating from one cloud service provider to another. A final scenario examines the risks linked to barriers to expansion for hyperscalers' competitors.

A. CROSS-CUTTING COMPETITIVE RISKS

393. The risks highlighted by the investigation relate to the imbalance in relations between hyperscalers and their customers (1), and to hyperscalers' cloud credit and egress fee practices (2).

1. UNBALANCED RELATIONS BETWEEN HYPERSCALERS AND THEIR CUSTOMERS

a) Customers, even key accounts, have limited capacity to negotiate contracts

394. Account creation and contract signature generally take place online[272], without the option of negotiation (see Part I.D). Only key accounts have certain, albeit limited, room for negotiation. One customer noted that "*many clauses in hyperscaler contracts are non-negotiable*". Another stated that "*contracts from providers of cloud products and/or services are generic and not customised*".

395. Few global customers are able to sign a contract containing negotiated clauses, whether on price, regulatory obligations, rebates or other financial elements. On this subject, one key account customer pointed out that "*practices are not standardised and will vary from one service provider to another. When dealing with hyperscalers - particularly American ones - it is generally more difficult to negotiate terms*". It added that "*for the moment, IaaS/PaaS providers are more incentivising in their proposals. They want to encourage as many*

[272] Contract available on this link. In addition, standard *service level agreements* (SLAs) are available here.

potential customers as possible to move to them. As a result, they offer solutions with partial, low-cost introductory prices."

396. But even key accounts find it difficult to negotiate, as confirmed by a business association, which noted that whatever "*their size, companies have little room for manoeuvre vis-à-vis major providers*". Uncertainty about future consumption of cloud services also prevents customers from making firm commitments to defined, pre-negotiated volumes. However, this is usually how customers apply for price reductions. For this reason, the general pricing principle for cloud services remains pay-per-use.

397. In its May 2021 report, the *Haut Comité Juridique de la Place Financière de Paris* therefore highlighted the significant imbalance in contractual relations between cloud service providers and their customers, in favour of the former, "*due to their economic power and technological expertise*", which creates "*a two-fold asymmetry between these providers and their customers*"[273]. Even major customers, such as banks, would be at a disadvantage in negotiations: "*in this context, the contractual balance of power between cloud providers and banks is sometimes likely to be unbalanced, and banks may find it difficult to negotiate the inclusion of certain contractual stipulations that meet regulatory requirements, particularly with regard to outsourcing*"[274]. This imbalance is due to the fact that high barriers to entry and/or expansion make these players "*de facto unavoidable*"[275].

398. In addition, cloud service providers can sometimes unilaterally modify clauses during the course of contracts. Some players indicated that the clauses modified in this way would relate to the following: "*reducing provider obligations via URL, changing the default contractual hierarchy, changing the financial commitment authorisations, etc.*" In this way, certain providers could unilaterally modify the scope of their obligations by simply referring to a website address. A key account customer also reported that it had experienced a substantial price increase from its provider, without receiving any justification.

399. Over and above this general difficulty in negotiating contractual terms with hyperscalers, the investigation revealed that it is difficult for customers to anticipate future costs.

b) Difficulty for customers to anticipate future costs, given the complexity of the offerings and the lack of pricing transparency.

400. The investigation carried out for this opinion showed that customers find it difficult to anticipate their future costs at the time of contracting, notably due to the complexity of offers and the lack of pricing clarity. Some providers, who already enjoy the advantages described above (strong investment capacity, ecosystem and/or conglomerate structures, etc.) (see Part II), could therefore be encouraged to make their prices less transparent and/or offer customers integrated packages in a non-transparent way, which would artificially raise prices and make these customers captive to their cloud environment.

401. Firstly, the investigation revealed that customers would not have access to the information that certain services are in fact complementary, leading to several services actually being

[273] Haut Comité Juridique de la Place Financière de Paris, "Rapport sur le Cloud bancaire: état des lieux et propositions", May 2021, page 22.

[274] Haut Comité Juridique de la Place Financière de Paris, "Rapport sur le Cloud bancaire: état des lieux et propositions", May 2021, page 23.

[275] Haut Comité Juridique de la Place Financière de Paris, "Rapport sur le Cloud bancaire: état des lieux et propositions", May 2021, page 23.

consumed and therefore sold together. AWS indicated, for example, that certain services are sold jointly because one service is designed to enhance the functionality of the other, such as Amazon EMR, which is sold with certain computing services (e.g. Amazon EC2, Amazon EKS, AWS Outposts, Amazon EMR Serverless). This complementarity may be justified from a technological point of view, but the information on the link between these services is not very transparent, as it does not always make it possible to take into account the fact that they require the use of related services. One customer gave the example of a computing service that requires the use of complementary network services. However, the prices for these related services are not clearly indicated by some providers.

402. Secondly, given the opacity of the prices, or at least their lack of clarity (see above), providers could have a strong incentive to boost their attractiveness by highlighting short-term gains for customers while ensuring their profitability through medium- and long-term usage conditions. This is the case, for example, when providers offer bundled services that include a number of services that are "free" but linked to underlying and complementary purchases in a way that is less easy for customers to decipher[276]. Once relationships have been established, providers may have an incentive to offer high prices on high value-added products, while making competition for new demand as unobjectionable as possible outside their own environment. As one customer stated, "*IaaS and PaaS providers offer very large catalogues of services and try to capture their customers by offering them high-level functionalities (platform level, as opposed to basic level) that are not available from competitors. This is a commercial approach based on the construction of offers that include very high-level services*".

403. As a result, this situation creates an imbalance in relations between providers, in particular hyperscalers, who have particularly varied and attractive catalogues, and first-time customers, who have no real vision, when choosing their provider, either of the services they will use in the future, beyond initial use cases involving relatively simple services (e.g. storage or computing capacity), or of the scale of their consumption. However, the purchase of cloud services involves a degree of uncertainty regarding the costs incurred for future purchases of services complementary to those purchased.

404. As a result, the imbalance in relations between hyperscalers and their customers entails competitive risks, insofar as hyperscalers could exploit this imbalance to attract customers to their offers, foreclose markets or exclude certain providers, raising barriers to expansion for smaller players.

2. CLOUD CREDITS AND EGRESS FEES

405. Cloud credits (a) and egress fees (b), whose principles have already been presented (see Part I.D), are two practices that have been analysed in depth by the *Autorité*. As a result, both individually and taken together (c), these practices need to be monitored more closely, as they illustrate the ability of hyperscalers to implement practices that differentiate them from

[276] The information collected during the investigation tends to show that several providers offer free services below a certain level of consumption ("free tier") (see, for example, the free offer from AWS (link), certain network services, internal data transfer, etc.) but also, for some, additional services (migration assistance, interventions by architecture or security experts, training days, support services, etc.). These services may be advertised to attract customers, but in reality require the purchase of specific services, or for a certain volume, which in reality ensure the remuneration of the provider. This issue is similar to that described for cloud credits (see below).

those of other providers, to their own advantage, and may limit competition for the workloads of companies already using these hyperscalers' infrastructures. Measures to regulate these practices are currently under discussion within the European Union and in France (see Part I and Part VI).

a) Cloud credits

406. As a reminder, cloud credits are trial offers in the form of service allowances offered by a provider and granting free access to a customer within a defined period. In practice, unlike a free trial, it is a sum to be spent in the form of an invoice credit granted before use (see Part I).

407. In its aforementioned Opinion 23-A-05, the *Autorité* found that cloud credits are likely to generate efficiency gains for many companies. First and foremost, they represent a means of facilitating migration or access to the cloud for customers for whom uncertainty regarding the suitability of the service for their needs would represent an obstacle. As one provider explained: "*Credits help attract inexperienced new customers to the cloud by making it easy to experiment with cloud services with limited risk* [...]*, make cloud services more affordable for specific types of customer, and encourage existing customers to try out new services and technologies*". In addition, choosing to move to the cloud can generate high costs, so it could be more efficient from a global perspective for providers to participate in the funding of this migration if they have the capabilities. In this respect, cloud credit offers seem to be particularly useful for the development of startups, since they give them easy and inexpensive access to cloud technologies, which are often essential to their growth.

408. The *Autorité* considers that cloud credits offered in the form of tests do not appear *a priori* to raise competitive risks, but those offered in the form of support programmes could be the subject of particular attention.

409. For cloud credits offered in the form of tests, one customer explained that "*the amount of these credits is not used for production. It simply allows operational staff to test new solutions*" and so "*does not represent a barrier to market entry*" in the long term. One *hyperscaler* confirmed that a credit of a few hundred dollars "*represents a very small amount compared to the costs of the cloud, and is designed primarily to enable customers to try* [the product/service] *and see if it meets their needs*".

410. For cloud credits offered in the form of support programmes, the total volumes of credits granted and the duration of use are both substantial and disparate between providers, which may give cause for concern. Hyperscalers claim to make proportionate use of cloud credits for the benefit of customers, enabling them to test different functionalities at lower costs before making a choice. On the other hand, providers other than hyperscalers denounce the high level of cloud credits offered by hyperscalers, which they feel they are unable to match and which, in their view, hampers the smooth operation of the market.

411. The ability of a competing provider "as efficient"[277] as the companies offering cloud credits to enter or remain profitable in this (or a related) market is questionable, given the amount of cloud credits offered by hyperscalers and the relatively major investments required for smaller providers. In other words, the question is whether cloud credits, combined with substantial investment, can act as barriers to entry or expansion for companies that are at

[277] "Just as efficient" in terms of variable costs.

least as efficient. This question needs to be assessed in the light of the different economic effects at work in this market, particularly in terms of size and range.

The presence of scale and range effects

412. As in other industries, the cloud market is only developing at the cost of heavy investment (see Part II). To determine a competitor's ability to enter the market, it is first essential to consider the minimum customer volume required (economies of scale) for a player to emerge and hold its own (profitability time horizon), and the influence of credit programmes on this critical mass and profitability time horizon. Cloud credit programmes target customers at a time when they are making long-term structural choices. The imbalance in the attractiveness of different providers' offers "*would deprive [smaller] providers of fair access to the market for startups in the creation or growth stages*". Part of the customer base would therefore be inaccessible to smaller players, limiting the entry and expansion of competitors. As a result, hyperscalers' credit programmes can lead to an increase in the time horizon required for a competing cloud service provider's business to become profitable.

413. In addition, the presence of players such as hyperscalers, which are active in various related digital markets (cloud and office software, for example), raises questions about the ability of credit programmes to link the consumption of products and services from the same provider in different market segments, within a diversified offering.

414. Scale and range effects also depend on the provider's financial capacity and the profitability of credit offers. According to one hyperscaler, the future income generated by the cloud credits granted to customers far exceeds their initial cost. It claimed that credit programmes are "*profitable and generate a positive return on investment in the medium term (generally three years), if not sooner*". However, it is not certain that a new entrant to the cloud sector, which is as efficient in terms of variable costs as the hyperscalers, but does not enjoy the same scale and range effects as the established providers, will be able to make such a discounted sales policy profitable in such a short space of time.

Impossible to replicate cloud credit offers identically

415. While hyperscalers are able to offer generous credit programmes, smaller, non-hyperscaler providers are not always in a position to compete (see Part I). For example, pure players face greater financial constraints that could prevent them from replicating credit offers. As the *Autorité* recalled in its aforementioned Opinion 23-A-05, "*If these forms of credit are offered by companies in a dominant position, over and above the possible capture of customers within a single cloud environment, they could have potentially anticompetitive effects, particularly on smaller providers who would be unable to replicate these offers profitably. They are therefore likely to raise barriers to the expansion of competing providers, subject to efficiency gains or objective justification*"[278].

416. According to one provider, the current competitive imbalance stems from a difference in scale between the players, as "*the more powerful the player, the greater the volume it can mobilise to offer credit. For technical reasons, this volume that can be mobilised is closely linked to the size of the player, since it depends on the percentage of its infrastructure occupied*". This finding is shared by some customers. One pointed out that "*hyperscalers are able to release credit "easily" given their size, which a new entrant would not be able to do*".

[278] Opinion 23-A-05, paragraph 57.

417. The public consultation revealed that many providers are not in a position to match the cloud credits offered by the biggest players, which would result in a significant loss of potential customers. This point is disputed by one hyperscaler, who argued that there is no competitive problem because "*the offering of cloud credits by providers is a common trade practice in the cloud sector, and the credit amounts* [it offers] *are limited and comparable to those offered by competitors*". However, while the amounts of cloud credit offers are often relatively comparable between hyperscalers, they can be up to ten times higher than what is offered by smaller providers, and it is clear from the investigation that many of the latter either do not offer cloud credits or find it difficult to offer comparable credits to as many customers (see Part I.D). According to one cloud service provider, the cloud credits offered to startups by hyperscalers are "*distortions of competition, as it is impossible for small or even medium-sized operators to match them*". Another said that it is a "*financial barrier to entry*", because "*it is very difficult, if not impossible, for smaller players to offer the same amounts*". Lastly, another pointed out that "*large amounts of cloud credit are often demanded by the customers we contact, who ask us to match the trade practices of the market leaders, which a small provider is financially unable to do*". If some providers, other than hyperscalers, manage to match the face amounts of cloud credits offered by hyperscalers, they would probably not be able to offer them to the same number of customers.

418. The investigation revealed that, in some cases, cloud credits are granted to customers conditional on substantial purchase commitments or volumes. This is the case, for example, with the "Activate" programme, aimed at startups, and the "Migration Acceleration" programme, both offered by AWS. For hyperscalers, these credit programmes are justified in two ways. First, they help pass on cost savings to providers for larger and less uncertain consumption quantities in the cloud sector. Second, they are a means of providing discounts to offset the costs of migrating a customer's workloads from their on-premise facilities or from a previous cloud service provider to its products and services. This could offset the costs of transferring data or training customer teams on the new products and services offered by the provider. Some providers justify the existence of cloud credits as "*one form of discount among others*", as observed and "*widely accepted in many sectors*".

419. Many customers see cloud credits as a price-cutting element. Therefore, according to one, what counts is "*not the price reduction mechanism used (cloud credits or other), but the overall unit cost reduction (taking into account all the price reduction mechanisms to be applied to the provider's initial price, which is not subject to negotiation)*". For another, "*the whole commercial effort*", which includes cloud credit programmes, is taken into account in its choice.

420. An important difference with the practice of loyalty rebates generally observed by the *Autorité*[279] is that cloud credits allow goods or services to be consumed completely free of charge. In a situation where a contestability of demand problem is identified, this would be an extreme case of loyalty rebates on the totality of volumes and invoiced price, or even a predatory practice.

[279] For example, Decisions 16-D-11, 15-D-20 and 09-D-04.

Cloud credit as part of a customer lock-in strategy

421. The granting of cloud credits could be part of a more global strategy of locking in customers. This is because cloud credits are reserved for the use of the provider's products and services for a period of up to two years, against a backdrop of technical and price barriers to migration (see - b below). In the words of one provider, "*cloud credits are not just about testing their platform or offsetting migration costs, but about buying their customer base and locking in the market*". The financial costs of change associated with the specific investments made by customers previously attracted by disproportionate credit volumes would then lock them into the ecosystem of the major providers. One customer found that "*once a cloud provider has been chosen, a company has to invest to make it work and be able to use the cloud. It is therefore not easy to invest again to change provider.*" For a customer, the cost of changing provider after using the credits offered would be proportionate with the investment made and therefore depend on both the amount and the duration of the credits offered.

422. This strategy is causing concern among some providers. In particular, they fear that they will not have access to companies perceived as strategic due to their high development and innovation potential, such as startups, or that customer choice will be distorted. Cloud credits would encourage "*users to choose cloud services not on the basis of objective criteria linked to their needs, but solely according to the number of credits they are granted*". The investigation also revealed that large companies appear less sensitive to and dependent on cloud credit programmes than startups. One pointed out that "*these credits* [...] *are relatively limited and do not influence the final choice of provider*". Another declared that "*while cloud credits are part of the discount, they are not the main point of* [its] *choice of cloud*".

423. So, even though cloud credits are likely to generate efficiency gains for many companies, they need to be given special attention. The high amounts sometimes proposed, the vast ecosystem of companies they cover, their validity periods and the lock-in risks described above 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 service providers to respond.

b) Egress fees[280]

424. As seen earlier (see Part I), a number of hyperscalers have set up a cloud service provision model based on charging customers for the volume of data leaving their environment ("egress-only pricing model"). These external data transfers can go from the provider's data centre to the data centre of another cloud service provider in the event of multi-cloud use requiring data transfers[281] or definitive migration to this other provider. They also cover data transfers to the customer's on-premise facilities in the event of hybrid use[282] or definitive localisation of data on-premise, or to its end-users as part of its day-to-day operations[283].

425. The investigation showed that hyperscalers pass on a significant proportion of their costs to these egress fees (i.e. "outgoing" billing for costs linked to data centres, servers, optical

[280] "Egress" means *the act of going out or leaving a place* (source: Oxford languages).

[281] This would be the case, for example, for a company whose data is hosted by cloud service provider A, and which is looking to use the analytics services of cloud service provider B.

[282] Concurrent use of public cloud services and on-premise services (on-premise or private cloud).

[283] This would be the case, for example, for a streaming service whose content is hosted in the cloud.

fibres, bandwidth, etc.). In reality, however, these numerous costs are common to all the different services offered by a cloud service provider. They could therefore be covered just as well by storage or computing fees, which are by nature more predictable since they are independent of traffic, unlike egress fees, whose pricing structure is proportionate with the volume of data transferred. As a result, customers are unable to anticipate future data traffic requirements in advance, and egress fees are now a challenge for customers wanting to migrate workloads from their primary providers' environments when these providers are invoicing for them, and for those wanting to set up an integrated multi-cloud architecture rather than one compartmentalised into silos[284]. This pricing scheme also enables *prima facie* reductions in the price of cloud services (*i.e.* storage, computing power, etc.) for customers choosing their first cloud service provider.

Fears of lock-in and difficulties expressed by customers, particularly in anticipating costs

426. As confirmed by the vast majority of the stakeholders questioned, charging these fees on outgoing traffic, which is increasing significantly in view of the ever-greater volumes of data circulating, entails a risk of customer lock-in, and could therefore have a direct negative impact on the long-term growth potential of customer companies.

427. Firstly, when contracting with their cloud service provider, it is difficult for these companies to anticipate their future data transfer requirements. In addition, despite the publication of pricing grids, egress fees are difficult to anticipate due in particular to their pricing structure, which is proportionate with the gigabytes transferred. Customers are therefore unable to anticipate the costs involved. On the other hand, the cloud market is still developing against a backdrop of the first-time migration of French companies, and this migration is slower in France than in the rest of Europe (see above). So, when making this choice, many customers, whose deployment in the public cloud is still limited, are not necessarily considering a future change of provider or the use of a multi-cloud architecture, and therefore give relatively more weight to the short-term cost represented by the fees for the different cloud services (including cloud services for storage, computing power, etc.).

428. By shifting a significant part of the network cost to egress fees, cloud service providers can reduce the price of their offerings. Combined with the granting of cloud credits for these same services, this makes it possible to offer particularly attractive contractual terms - which smaller alternative providers cannot replicate (see above) - to corporate customers who have difficulty understanding the long-term impact of egress fees on their business model.

429. For these reasons, customers do not put much different providers in competition with each other in terms of their egress fees.

430. Secondly, if customers of cloud services are faced with high egress fees in the event of data migration, they will be encouraged to stay with their original provider. For example, a company that has already migrated an initial workload to the infrastructures of a hyperscaler will incur significant egress fees if it migrates it from its primary provider to another provider. Similarly, the same company will incur significant data transfer costs if it migrates subsequent workloads to other providers and develops a multi-cloud architecture requiring data exchanges between workloads. In other words, as they are currently structured, these fees may create a risk of customer lock-in, by making it more difficult for customers to leave

[284] Given the existence of these transfer costs, current multi-cloud uses are limited to those, in silos, that require very little data exchange.

their primary provider as well as use several providers at once, in an integrated way, i.e. for the same workload or for different workloads when they involve recurring data transfers between them.

431. One French key account illustrated the risks of locking in egress fees: *"Egress fees have several consequences. First, high egress fees can have an impact on a customer's strategy in relation to its decision to migrate from one cloud provider to another, and on how to implement a possible migration. Second, egress fees can also arise for the customer when using tools that are not on the cloud and need access to data located on the cloud to work (for example, to process certain raw data put on the cloud), which can discourage a customer from using non-cloud tools. Nor does it encourage multi-cloud solutions, with applications spread across several clouds (too many data exchanges). The "egress only" cost model is designed to encourage customers to put their data in a single cloud and compute, view and process it on the cloud to avoid additional costs. Egress fees are all the more worrying for customers as cloud providers are asking their customers for an increasing commitment in terms of spending in order to qualify for price reductions; this is pushing companies to put more and more data on the cloud with a high degree of uncertainty over the total cost of subsequently extracting the data*".

432. The American[285], Dutch[286], British[287] and Japanese[288] authorities have also identified a risk of competitive distortion linked to the development of these pricing models.

Pricing not justified by technical or economic reasons, but rather the result of a commercial strategy

433. The *Autorité* considers that the various economic and technical explanations put forward by the major cloud service providers, who charge their customers substantial egress fees, do not justify the pricing method used.

434. The interested parties argue that these fees enable them to recover their costs and make their investments in infrastructure profitable, thus enabling them to offer their customers high levels of reliability, resilience, security and performance.

435. The cost would cover investment in data centres (buildings, land, servers, network equipment, etc.) and in the deployment of fibre optic links and submarine cables enabling data transfers over short and long distances, as well as the different operating and maintenance expenses (continuous power supply, 365 days a year, system cooling, monitoring, data encryption). These spending levels would not be replicated by non-hyperscaler cloud service providers, who have not deployed such infrastructures and rely on third-party bandwidth providers, whose rates are lower but who cannot guarantee the same quality of service levels (performance, resilience, security, etc.).

436. However, the information collected during the investigation did not corroborate these arguments.

437. On the contrary, it appears that the structure (*see sub-section below*) and levels (*see sub-sections below*) of the egress fees charged by hyperscalers to their customers do not reflect,

[285] "*Investigation of competition in digital Markets*", Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary, 2020.

[286] ACM Cloud Services Market Survey, 5 September 2022, p. 18.

[287] "*Cloud services market study*", Call for input, Ofcom, 2022.

[288] https://www.jftc.go.jp/en/pressreleases/yearly-2022/June/220628_2EN.pdf.

in a transparent and predictable way for the latter, the costs directly incurred for data transfer outside the networks. This pricing scheme could be at the root of the difficulties expressed by customers in anticipating costs. Furthermore, contrary to what hyperscalers suggest, the price difference between incoming and outgoing traffic is essentially the result of a commercial strategy and is not explained by technical reasons (see *subsection below*).

438. Lastly, the hyperscalers' argument that transfer fees could not be part of a commercial retention strategy, since they apply uniformly to all types of outgoing data transfer - i.e. both transfers to a competing provider's infrastructure and transfers to the Internet (i.e. outside competing providers' environments), as is the case for certain common transactions[289] - does not dispel the risks identified (see *subsection below*).

Pricing structure not necessary to recover network costs

439. According to some stakeholders, the very structure of these prices, based on the quantity of data transferred and not on peak bandwidth is at the root of the difficulties expressed by customers in anticipating their costs and the high margins achieved by hyperscalers.[290] In their view, the network cost (*i.e.* the cost of bandwidth) actually incurred by cloud service providers charging egress fees would be a fixed cost linked to the maximum simultaneous data transfer capacity on the fibre links, i.e. the "diameter" or "throughput" of the bandwidth[291]. In other words, this cost would be explained by the maximum throughput allowed by the infrastructure and not by the total amount of data transferred by customers over it[292].

[289] Data transfer on-premise or to the end users of a customer company, for example.

[290] See Clouflare's 2021 study (https://blog.cloudflare.com/aws-egregious-egress/), in which the cloud service provider estimates the margins achieved by AWS in Europe and the US/Canada for the use of "transit" networks at almost 8,000% (transit providers enable data to be sent to any other network on the Internet, and are used by major cloud service providers for interconnection with third-party networks on the Internet). It should be noted that this estimate is based on Cloudflare's internal estimates of the cost of third-party bandwidth in each region of the world. Cloudflare also suggests that the margins achieved by AWS could be even higher when transferring data to other cloud environments that offer direct and settlement-free interconnection, for which AWS bears no marginal bandwidth cost (i.e. zero wholesale transit price).

Cloudflare argues lastly that the fixed costs associated with investments in data centres, optical fibres and other network equipment are relatively limited compared to the levels of egress fees charged by hyperscalers like AWS, given on the one hand the particularly large scale effects they enjoy and, on the other, the significant decline in IT equipment costs over time.

[291] As with telecoms networks, one of the main characteristics of cloud markets is the size of the fixed costs. In this respect, a telecoms operator, which markets services using telecoms infrastructures, in the same way as a cloud service provider, owns its networks, or leases capacity, not flow, on a third-party network to sell subscriptions and individual connections. In the telecoms sector, for example, bandwidth use on the wholesale market as well as on the retail market, for individuals, is subject to a flat rate (independent of traffic) proportionate with the maximum available bandwidth.

[292] See also the Cloudflare study cited above (https://blog.cloudflare.com/aws-egregious-egress/): "*AWS charges customers based on the amount of data delivered - 1 terabyte (TB) per month, for example. To visualize that, imagine data is water. AWS fills a bucket full of water and then charges you based on how much water is in the bucket. This is known as charging based on "stocks". On the other hand, AWS pays for bandwidth based on the capacity of their network. The base unit of wholesale bandwidth is priced as one Megabit per second per month (1 Mbps). Typically, a provider like AWS will pay for bandwidth on a monthly fee based on the number of Mbps that their network uses at its peak capacity*.

440. So, as pointed out by one French electronic communications operator providing bandwidth, "*network providers' invoicing is generally based on available bandwidth and the 95% percentile (Mbps), whereas cloud providers charge for outgoing GB*". Traditional telecoms operators, who also have bandwidth capacity at their disposal, charge certain cloud service providers and others for the useful 95th percentile use of their bandwidth, i.e. the available network capacity that their Internet operator needs to maintain in order to carry their customer's traffic unhindered 95% of the time.

441. In contrast, the major cloud service providers charge for the total amount of data transferred externally by their customers (generally not including the first 100 gigabytes transferred each month).

442. While hyperscalers as a whole maintain that this is standard trade practice for a cloud service provider, in reality, other providers charge relatively little or nothing for outbound traffic. The investigation revealed that some alternative cloud service providers, who have also invested heavily in hardware in the same way as hyperscalers, incorporate the cost of data transfers directly into the prices of their services *(*for example, in the price of data storage, calculation or processing) so that the costs they incur are no longer passed on to their customers on the basis of outgoing traffic. They offer different, predictable, flat-rate pricing models, i.e. independent of the number of gigabytes transferred or processed, which they claim cover the costs of infrastructure and bandwidth capacity.

443. According to one stakeholder interviewed, French cloud service providers who charge egress fees have reduced the level of their transfer fees. Furthermore, to differentiate themselves from the hyperscalers, some American players are no longer charging egress fees and are instead proposing a new flat-rate model for network usage. For example, in 2018, Wasabi announced it would end egress fees and include its network costs in a flat fee independent of the data flow of its storage service[293]. In 2021, Cloudflare announced its new storage service ("object R2") with no egress fees charged for data output and offered a support tool to gradually move data out of the environments of players who charge such fees in order to spread the cost over time[294].

444. Such a pricing structure, independent of the amount of data transferred, could promote the transparency of the costs ultimately incurred by corporate customers and enable them to change provider. In addition, it could further increase the contestability of cloud markets, which are characterised by significant technical limitations in terms of interoperability and portability (see B below). Admittedly, in the short term, these fixed-price models offer customers the advantage of predictability, since the cost no longer varies according to traffic, but they do not make it possible to offer storage or computing prices as competitive as those offered by hyperscalers, which, conversely, artificially allocate a significant proportion of their costs to outgoing data flows. However, in the longer term, given their advantages in terms of predictability and comparability, they could facilitate and even stimulate the contestability of public cloud service markets, resulting in greater competition.

[293] https://www.techtarget.com/searchstorage/news/252438039/Wasabi-Technologies-eliminates-cloud-storage-egress-fees.

[294] https://blog.cloudflare.com/introducing-r2-object-storage/.

Figure 18 - Comparison of egress fees expressed in USD or EUR and invoiced in Europe in 2022 for each GB transferred, by the main public cloud service providers in France

		Azure[295]	**AWS**[296]	**GCP**[297]	**OVH**[298]	**Oracle**[299]	**Scaleway**[300]
Ingress Fees (cloud entry)		Free	Free	Free	Free	Free	Free
Transfer within the same cloud	Same region	$0.01	$0.02	$0.01	€0.01	Free	Free
	Same continent	$0.02	$0.02	$0.02	€0.01	Free	Free
	Outside the continent	$0.05	$0.02	$0.08	€0.01	Free	Free
"Egress Fees" (exit to the Internet)	First 100 GB	Free	Free	$0.085	€0.01	Free	Free[301]
	Next 10TB	$0.087	$0.09	$0.085	€0.01	Free	€0.01
	Next 40TB	$0.083	$0.085	$0.065	€0.01	$0.0085	€0.01
	Next 100TB	$0.07	$0.07	$0.065	€0.01	$0.0085	€0.01
	Next 350TB	$0.05	$0.05	$0.065	€0.01	$0.0085	€0.01

High egress fee levels that do not reflect the costs directly incurred for bandwidth use

445. The information collected during the investigation tends to show that the bandwidth cost incurred by a cloud service provider in reality represents only a minority proportion of the total cost incurred in providing its services.

446. So, according to some of the stakeholders interviewed, the share of network costs in a provider's total costs is generally around 10%, with bandwidth costs representing only a sub-part of total network costs (capital and operating expenses linked to fibres, data centres, servers, etc.).

447. Furthermore, the statements made by the different stakeholders interviewed overwhelmingly point to a significant drop in network costs in France and worldwide over the past few years (although the overall invoice for bandwidth users has risen, given the growth in traffic circulating). One electronic communications operator in France, itself a bandwidth provider, commented: "*There is a significant erosion of network prices in France and worldwide. The*

[295] Azure bandwidth pricing; data collected on 4 April 2022. The egress fees used correspond to the prices for output to the Internet routed via the Microsoft Premium global network. Internet Egress, routed via Routing preference transit ISP network, is charged at **$0.08** per GB for the first 10 TB, **$0.065** per GB for the next 40 TB, **$0.06** per GB for the next 100 TB and **$0.04** per GB for the next 350 TB.

[296] Amazon EC2 on-demand pricing; data collected on 4 April 2022.

[297] Estimates made by ACM in its market study, as egress fees were no longer available on 4 April 2022 on the Google Cloud networking pricing page (link).

[298] OVHcloud Storage pricing; data collected on 4 April 2022.

[299] https://www.oracle.com/fr/cloud/networking/pricing/; data collected on 4 April 2022. "*Oracle Cloud infrastructure offers low networking prices that enable customers to move significant quantities of data for less. Inbound data transfer is free, and we offer a high threshold for free outbound data transfer—the first 10TB free for each regional zone or product SKU. After that, outbound data transfer rates are based on geography. Rate differences across geographies differ due to variable carrier rates.*"

[300] Scaleway prices data collected on 24 October 2022.

[301] The first 75 (not 100) GB transferred each month outside the Scaleway network are free.

price of IP transit has fallen steadily over the last ten years". According to Cloudflare's 2021 study[302], wholesale prices for data transit services have fallen by an average of 93% over the last 10 years[303], while the egress fees charged by AWS have fallen by just 25%[304]. The evolution of the egress fees charged by hyperscalers would therefore only slightly reflect this reduction in the unit cost of bandwidth.

448. Despite these minority and declining network charges, the information collected by the investigation services revealed that egress fees can sometimes make up the bulk of a cloud service customer's invoice, while bandwidth charges are not the main cost centre for the cloud service provider. Furthermore, while unit costs may seem moderate (catalogue prices at the end of 2022 varied from 8 to 9 cents per gigabyte for the first 10 terabytes downloaded by customers), they can soon represent particularly high amounts for a company, especially when its workloads require significant data transfers between different infrastructures (cloud and/or on-premise).

449. For example, the outbound bandwidth revenues of one of the major providers surveyed increased more than sixfold in France between 2018 and 2021, when its total cloud service revenues over the same period increased only threefold. Another major cloud service provider surveyed saw outbound bandwidth revenues represent up to 15% of its total cloud revenues in France between 2018 and 2022, while overall network costs - of which outbound bandwidth is just one cost item - already account for a smaller proportion, around 10%, of a hyperscaler's total costs (see above). These fees, linked solely to the outbound transfer of customer data, generate monthly revenues of several million euros for a hyperscaler in France.

450. In addition, the claim by some major providers that they do not make a profit on these transfer fees could not be confirmed. One hyperscaler interviewed by the investigation services stated that direct expenses related to the exploitation of the bandwidth used by its customers, worldwide, amounted to several tens of millions of dollars in the 2022 financial year. Over the same period, it received several hundred million dollars in egress fees, a very substantial apparent margin.

451. The evidence collected during the investigation suggested that the level of egress fees appears to be disconnected from the costs actually incurred for the sole use of bandwidth for outgoing cloud flows, and showed that in reality, hyperscalers pass on a significant proportion of their network costs (data centre, servers, etc.) to the output of each gigabyte.

452. Lastly, as mentioned above (see Part II.A.), hyperscalers benefit from very significant economies of scale and scope, enabling them, with the help of a large and diverse customer base, to recoup the essentially fixed costs of their networks, which are based not on total demand activity but on peaks in activity. Such competitive advantages should *a priori* benefit their customers in terms of both cloud services and data transfers. However, the investigation revealed that despite these significant scale and range effects, and due in particular to this asymmetrical allocation of many costs to data output, the egress fees of the three hyperscalers are much higher than those of alternative cloud service providers (up to

[302] https://blog.cloudflare.com/aws-egregious-egress/.

[303] The cost of data centres, fibre and other network equipment has also fallen at a similar rate, according to Cloudflare.

[304] This drop in AWS egress fees observed by Cloudflare could be explained, among other things, by the new free offers on the first 100 GB of data transferred each month by hyperscaler customers (see above).

ten times higher), who also have hardware infrastructures, but a smaller and less diverse customer base.

A price difference between incoming and outgoing traffic resulting from a commercial strategy

453. According to some major cloud service providers, charging for outgoing traffic would enable customers to pay for the actual, recurring use of outgoing bandwidth, and guarantee pay-as-you-go pricing. Conversely, free incoming data transfers would be justified by the one-off, non-recurring nature of the cost borne by the provider, which can easily be incorporated into the prices of cloud storage services, for example. This asymmetry in price construction would, on the one hand, support migration to the cloud and, on the other, ensure that customers who store but never transfer data, incur no additional costs.

454. However, the actual cost of bandwidth for the cloud service provider, whether inbound or outbound, is related to the maximum throughput allowed by the infrastructure it uses, and not to the total amount of data flowing through it. Following the example of some other cloud service providers (see Figure 18), hyperscalers could choose to incorporate this fixed cost into the pricing of their cloud services, and charge their customers for neither incoming nor outgoing traffic, since the cost actually incurred is not traffic-dependent.

455. In fact, one hyperscaler confirmed that the only justification for the egress fee pricing structure was commercial: "*to charge both outbound and inbound at the same rate* [would] *make us less competitive with* [other public cloud service providers'] *offerings* [...] *technically speaking, there is no difference between inbound and outbound traffic, given that the costs are very high. The price difference* [paid vs. free] *is essentially commercial*".

456. In any case, a flat-rate pricing structure, *i.e.* one that is not proportionate with the amount of data transferred, would have been much clearer and more transparent for cloud service customers. It is very difficult for them to anticipate their future data consumption in advance when signing contracts, even supposing that the level of egress fees is a transparent part of the contract.

The uniform application of egress fees to all outgoing transfers does not eliminate the risk of lock-in

457. According to some of the hyperscalers interviewed, charging egress fees uniformly on all outgoing transfers does not reflect a customer retention strategy. Indeed, hyperscalers could only observe a transfer from their network to the Internet without knowing either the destination or the purpose, and would therefore not have the technical capacity to differentiate "ordinary" uses of their cloud services from uses that involve recourse to a competitor, such as multi-cloud uses or definitive data migrations, as "*network protocols do not allow a distinction to be made between traffic for the purposes of data migration and ordinary traffic*".

458. According to one of these hyperscalers, the vast majority of these transfers are linked to the "ordinary" use of its cloud services and not to multi-cloud uses or definitive migrations, as every time an Internet user consumes content deployed on the cloud, the distributor of this

content, which uses the bandwidth of its cloud service provider, incurs significant outgoing costs.[305]

459. Firstly, however, it appears from the investigation that cloud service providers actually have a range of technical solutions at their disposal to determine the destination of the traffic leaving their infrastructures[306].

460. Secondly, the assertion that a hyperscaler's egress fees mainly concern data transfers linked to the continuous and recurrent use of outgoing bandwidth by its customers (such as Netflix, for example, which broadcasts large streams to its end users), and not to multi-cloud uses or data migration, is not sufficient to demonstrate the absence of competitive risk linked to such practices. Conversely, the absence or insufficiency of traffic from multi-cloud uses or linked to data migration could corroborate the existence of a significant barrier effect on the possibilities of data movement outside hyperscaler environments and on the degree of contestability of cloud markets.

c) Cloud credits and egress fees limit competition on hyperscaler customers' workloads

461. In the *Autorité's* view, cloud credits and egress fees should be subject to closer scrutiny due to the competitive risks they entail, whether considered separately or together (see Figure 19).

462. Since many cloud service providers claim that they are unable to match the massive cloud credit offers made by hyperscalers, great care must be taken to ensure that the credit offers of operators who may be dominant in the cloud services market do not prevent any equally effective competitors from entering or expanding.

463. This vigilance is particularly crucial as cloud credit practices, which aim to attract customers to a provider by granting free consumption units for a limited period of time, are generally accompanied, in the case of hyperscalers, by pricing mechanisms such as egress fees designed to reduce the incentive to switch to a competing provider. Cloud credit programmes therefore reinforce the risk of lock-in already identified by the practice of charging for outgoing traffic.

464. In this respect, the *Autorité* considers that as they are currently structured, these transfer fees may create a risk of customer lock-in, by making it more difficult for customers to leave their primary provider or use several providers at once, in an integrated way, i.e. for the same workload or for different workloads when they involve recurring data transfers between them.

465. Given the importance of technical barriers to interoperability (see Part IV.B) and the intrinsic advantages of hyperscalers (see Part II), it is particularly necessary to ensure that these markets are as contestable as possible, otherwise the scope of competition could be limited

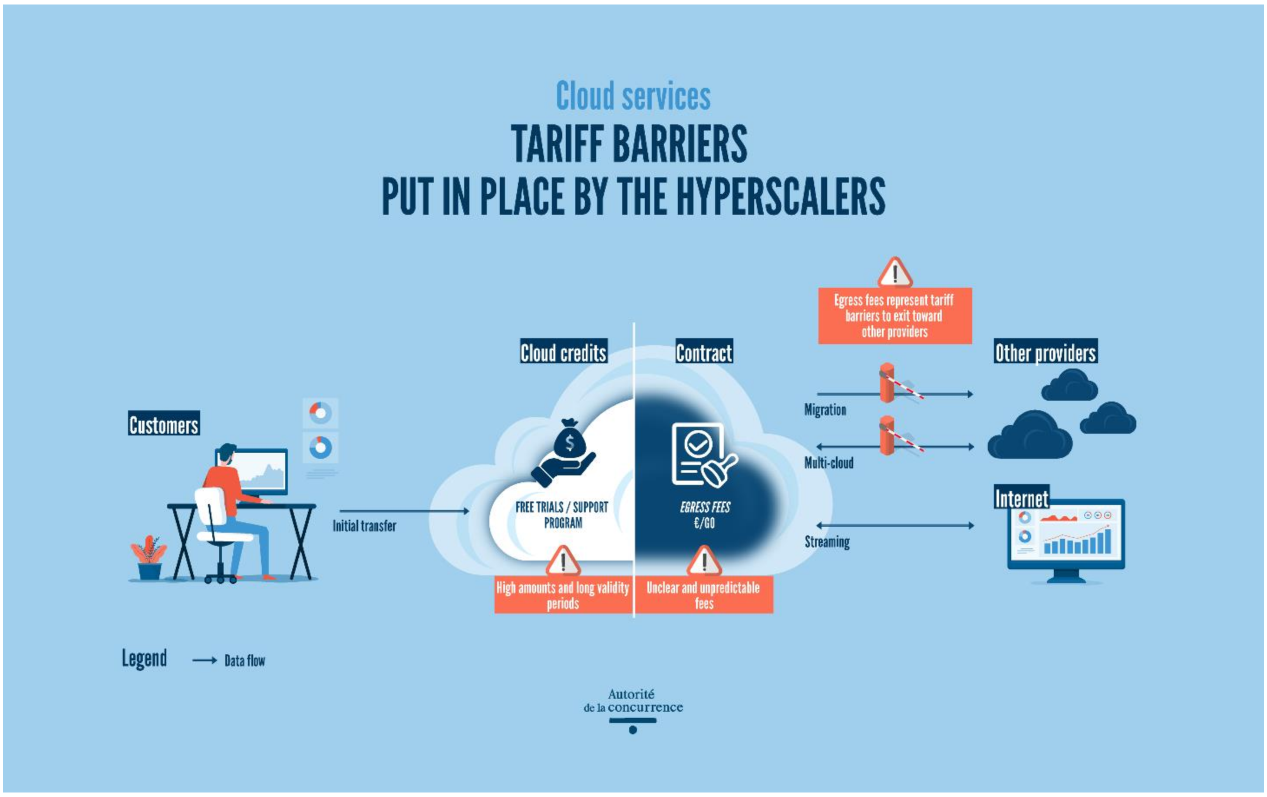
[305] For example, when a customer streams video content to its end users.

[306] A hyperscaler can find out the destinations of the traffic of some of its multi-cloud customers from their testimonials on the one hand, and from public information that indicates whether a company uses multiple cloud service providers, on the other. For example, information obtained from public registries, such as the Domain Name System (DNS), which translates IP addresses and domain names, controlling which server an end user will connect to when they type a domain name into their browser (query), can be used to determine the location of a customer's services. It would also be possible to access public information supplied by multi-cloud solution providers (such as Nutanix) who communicate their customers' achievements and use them as commercial references, to identify customers using more than one cloud service provider.

to winning over companies that have not yet migrated to the cloud, or to cloud native applications. Companies already present in the cloud would then eventually be exposed to the risk of price increases or a drop in the quality of their cloud services (resilience, security, performance, etc.).

466. In this respect, both the Data Act and the draft law to secure and regulate the digital space include provisions aimed, ultimately, at eliminating these egress fees to improve the contestability of cloud markets (see Part I and Part VI). In addition, a framework for cloud credits is provided for in the aforementioned French draft law (see Part I below and Opinion 23-A-05 above). Competition law and the law on restrictive trade practices could also be effective tools for analysing the effect of such practices on competition, particularly if implemented by a dominant operator (see Part V).

Figure 19 - Pricing barriers used by hyperscalers


Cloud services
TARIFF BARRIERS
PUT IN PLACE BY THE HYPERSCALERS
Customers
Initial transfer
Cloud credits
FREE TRIALS / SUPPORT PROGRAM
High amounts and long validity periods
Contract
EGRESS FEES
€/GO
Unclear and unpredictable fees
Egress fees represent tariff barriers to exit toward other providers
Migration
Multi-cloud
Streaming
Other providers
Internet
Legend
Data flow
Autorité de la concurrence

Source: Autorité de la concurrence

Cross-cutting competitive risks

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

Firstly, the imbalance in relations between customers and hyperscalers can be seen in the presence of certain key players 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 transparency.

Two pricing practices - cloud credits and egress fees - also caught the *Autorité's* attention.

Cloud credits allow customers to benefit from a spending reduction for certain eligible cloud services. Offer strategies are many and vary between providers. However, it is possible to group programmes into two broad categories, depending on whether the credits are intended for product testing and discovery, or for targeted business support.

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 service providers, who use them to spread and encourage the adoption of their technology.

However, the *Autorité* considers that special attention should be paid to targeted support offers. The sometimes high amounts proposed (up to 200,000 dollars over two years), 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 service 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 with the major providers on the market. This practice, which is causing concern in the market, 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 provider or using several providers simultaneously.

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

Egress fees are charges that customers have to pay for each data transfer outside their provider's infrastructure. They have mainly been set up by hyperscalers, who charge per outgoing bandwidth usage.

These fees apply when a customer seeks to migrate to a competing provider's cloud services, use different solutions in a multi-cloud architecture that requires data transfers, or when it transfers data to its own site or to its end users as part of its everyday operations.

The investigation has shown that these fees are potentially disconnected from the costs directly borne by providers. 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 future needs in terms of data traffic and bandwidth usage. As a result, egress fees are now an additional obstacle to migration from the environments of the primary providers who charge them, as well as to multi-cloud use.

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 use several providers at once, and in an integrated way, i.e. for the same workload or for different workloads when they involve recurring data transfers between them.

B. SCENARIOS INVOLVING SPECIFIC COMPETITIVE RISKS

467. The *Autorité* has identified specific competitive risks in three different scenarios. The first two depend on the nature of the cloud service customer's migration movement: primary migration to the cloud, i.e. the migration of on-premise information systems to the cloud (1), or migration from one cloud service provider to another (2). The last scenario concerns barriers to expansion for hyperscalers' competitors (3).

1. SPECIFIC COMPETITIVE RISKS ASSOCIATED WITH MIGRATING ON-PREMISE INFORMATION SYSTEMS TO THE CLOUD

468. Particularly given the difficulty of successfully migrating data and applications to the cloud, the incumbent software solution providers could leverage their established relationships with corporate customers to encourage them to migrate to their own cloud solutions. Before examining these practices (b), the *Autorité* will look at the technical and organisational obstacles they face (a).

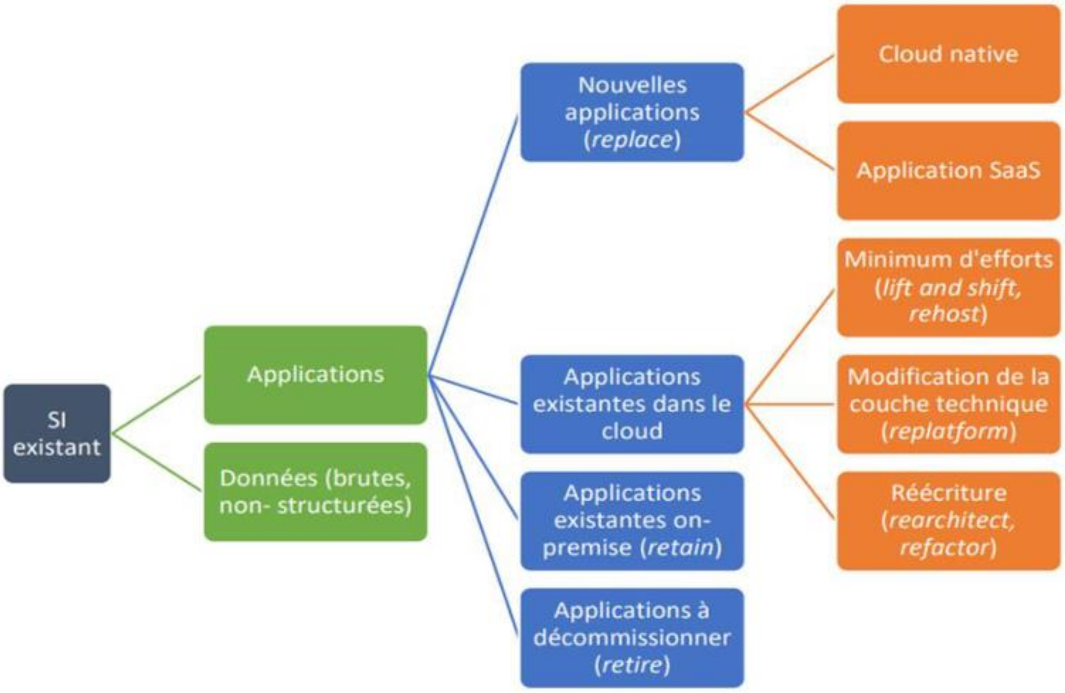
a) Technical and organisational obstacles to customer migration to the cloud which may encourage them to use incumbent providers

469. Traditional (non-cloud-native) companies need to ensure the interconnection of their different IT services with the cloud. This migration strategy is potentially complex, depending on the resources involved. Indeed, as Cigref points out, "*For most companies, the aim is not to migrate their entire IT to a cloud system, especially if it includes sensitive data*"[307].

470. Cigref illustrates the different choices available to companies when they decide to migrate data or applications to the cloud, using the following tree diagram.

[307] Above-mentioned Cigref report, page 16.

Figure 20 - Tree of possible decisions


SI existant
Applications
Données (brutes, non- structurées)
Nouvelles applications (*replace*)
Applications existantes dans le cloud
Applications existantes on-premise (*retain*)
Applications à décommissionner (*retire*)
Cloud native
Application SaaS
Minimum d'efforts (*lift and shift, rehost*)
Modification de la couche technique (*replatform*)
Réécriture (*rearchitect, refactor*)

Source: Cigref, Cloud migration strategies, a structural challenge for companies, pages 18 et seq. (link)

FR	EN
SI existant	Existing IS
Applications	Applications
Données (brutes, non-structurées)	Data (raw, unstructured)
Nouvelles applicatios (replace)	New applications (replace)
Applications existantes dans le cloud	Existing applications in the cloud
Applications existantes dans le cloud	Existing applications in the cloud
Applications existantes on-premise (retain)	Existing on-premise applications (retain)
Applications à décommissioner (retire)	Applications to be decommissioned (retire)
Cloud native	Cloud native
Application SaaS	SaaS application
Minimum d'efforts (lift and shift, rehost)	Minimum effort (lift and shift, rehost)
Modification de la couche technique (replatform)	Modification of the technical layer (replatform)
Réécriture (rearchitect, refactor)	Rewriting (rearchitect, refactor)

471. Migration to the cloud requires customers to make choices in the architecture of their information systems and applications:

– customers can choose to use specific services optimised for operation in a cloud environment to develop their applications. These are cloud-native applications, which differ from traditional company applications in that they are optimised to take advantage of the cloud environment (speed, flexibility) and can be easily scaled on different platforms[308];

- customers can also choose to adapt existing applications. Given that the applications used by the company were not necessarily developed to run on a cloud infrastructure, some modifications may be necessary. Customers can choose from several approaches depending on the characteristics of their applications:
  - they can first opt to migrate the application as it stands (the "lift and shift" approach);
  - or they can choose to completely overhaul the application (for example, by subscribing to a PaaS service offered by a cloud service provider who will manage the service) to adapt it to the cloud environment (the "refactor" approach); cloud service providers generally advocate this solution, as they can then offer their customers more innovative PaaS services optimised for their own cloud environment; customers, especially key accounts, seem to confirm the advantages of this approach;
  - they can also choose an intermediate approach, modifying only the application's technical layer (the "replatform" approach)[309].
- some legacy applications may not be transferred to the cloud, either because they are intended to remain on site (for sensitive data, for example), or because they will be phased out in the short to medium term.

472. Once this choice has been made, customers may need to manage data and applications across multiple environments (on-premise, private cloud, public cloud) and with multiple cloud service providers. In addition, customers' existing IT assets and architecture are sometimes difficult to integrate with the new cloud infrastructure, especially for the most innovative PaaS services (see Part II). One cloud player confirmed "*that many companies that have gradually migrated to the cloud now find themselves in practice with* [a] *patchwork of more or less hybrid multi-cloud infrastructure. Unlike companies that have developed their business directly in the cloud ("cloud natives"), the majority of companies existed before the development of the cloud and gradually migrated part of their business to the cloud as and when they needed to. For these customers, migration may have been carried out piecemeal, by activity or by process, resulting in the use of a multi-cloud solution that was not designed to be open or truly interoperable*". It is therefore common for companies to ask for support during the migration process, particularly from an integrator (see Part I.C).

473. In addition, these choices must take into account the ability of teams to cope with such transformations. According to one integrator, mastering cloud technologies and migration methods is not easy. This needs to change, especially as there is a clear decline in IT skills within companies. One customer told the *Autorité* that a managed database service alone had made it possible to avoid hiring a developer, which had resulted in significant savings for the company, the corollary being the lack of available skills to manage the migration. This finding was shared by a cloud service provider, who also noted a decline in IT skills in companies, affecting the negotiation, choice and mastery of their IT tools.

[308] https://aws.amazon.com/what-is/cloud-native/.

[309] https://www.redhat.com/en/topics/automation/what-is-it-migration.

474. More generally, migration to the cloud requires a change in corporate culture compared with an on-premise infrastructure, particularly in terms of security (network, rights management) and performance (transition from dedicated machines to shared resources).

475. Lastly, the companies concerned have deployed software that is closely interwoven with business processes and have therefore built up long-standing relationships of trust with software vendors. The complexity of migrating data and applications to the cloud can lead them to prefer their incumbent IT solution provider for the sake of simplicity and risk minimisation. One association of companies confirmed that "*the history of the IS is also important, as depending on the choices made in the past, certain solutions seem more appropriate than others (e.g. preference for Azure in the case of Microsoft history)*".

476. This finding is confirmed by the aforementioned ACM study, which highlights the influence of the historical choice of original IT service provider: "*Legacy firms often choose their cloud provider on the basis of IT products they already use.* [...] *A number of Dutch companies that already used the Office package from Microsoft, for example, state that they obtain it from a cloud provider, and are more likely to choose Microsoft Azure than another cloud provider*"[310].

b) Practices likely to limit customers' freedom of choice of cloud service provider

477. As explained above, some players, in particular incumbent software vendors, receive conglomerate advantages, including network effects, vis-à-vis customers who have installed their products on-premise (see Part II.D). They also maintain close relations with DSCs, which the investigation showed can play a prescriptive role when it comes to choosing a cloud service provider. These advantages could prompt some software providers to behave in a way that limits customers in their choice of cloud service provider.

Contractual restrictions on the free use in the cloud of software acquired on-premise from competing cloud service providers

478. Against a backdrop of unbalanced trade relations between cloud service providers and customers, characterised by the absence of negotiated contractual clauses, certain practices by cloud service providers who are also software vendors are likely to limit their customers' choice. Software vendors such as Microsoft and Oracle can leverage the advantage of their historical positions to launch and develop their respective cloud offerings and restrict the use of their software in a competing cloud.

479. As a result, the Commission has received several complaints concerning potential anticompetitive practices in the sector[311].

480. In particular, OVHcloud criticised Microsoft for licensing its products, such as Office, with contractual conditions that make it more expensive to use them in competing cloud

[310] Above-mentioned ACM market study, page 26.

[311] In all, four complaints have reportedly been filed with the European Commission against Microsoft; the first complaint was filed by OVHcloud in summer 2021 (see here). Other players have joined the complaint, including Aruba and The Danish Cloud Community. Nextcloud also filed a complaint against Microsoft in the same year. On 9 November 2022, CISPE finally announced that it had filed a complaint with the Commission against Microsoft for unfair software licensing practices. Lastly, Microsoft is also the target of a complaint to the Commission from Slack dating from July 2020; Slack, which markets its own internal messaging service, believed that Microsoft was abusing its dominant position by combining Teams with its other cloud software - Word, Excel, PowerPoint and Outlook (link).

environments. It is also alleged that Microsoft products do not perform as well as in other cloud environments. According to OVHcloud, Microsoft is using its dominant position on several upstream markets where its own products are present (PC operating systems, server operating systems and PC productivity software) to prevent competition in the related cloud and collaborative tools markets. These practices make competing cloud service providers less competitive while favouring Microsoft's own cloud solution, Microsoft Azure.

481. CISPE also denounced other practices against Microsoft: "*anti-competitive practices including unjustified and discriminatory bundling, tying, self-preferencing pricing and technical and economic lock-in, continue to be used by dominant software companies to restrict the choice of European companies as they move to the cloud. In particular, Microsoft uses its dominance in productivity software to direct European customers to its own Azure cloud infrastructure to the detriment of European cloud infrastructure providers and users of IT services*" [312].

482. One customer interviewed during the investigation confirmed the existence of restrictions on the use of Microsoft licences on a competing cloud: "*there is a warning on GCP* [Google cloud platform] *prohibiting the use of Microsoft Windows Server in BYOL* [bring your own licence[313]] *unless expressly agreed by Microsoft, and it is up to the customer to verify the existence of such an agreement. In all other cases, there is little indication that the Customer must check with each software publisher whether the licence conditions of the publishers concerned authorise the installation of their software in the cloud. For example, in the Google GCVE dedicated cloud, it was very difficult to obtain clear information on the provision of Windows Server licences for this environment. Some software vendors are contesting the possibility of using their software in the cloud without additional remuneration*".

483. In this regard, it is worth noting that following changes announced on 1 October 2022, Microsoft customers could now move their licences to a partner's cloud (not all providers are partners), use shared hardware and enjoy greater flexibility in their software licence

[312] See the summary of the complaint made by CISPE (link) and the report written by Frédéric Jenny for CISPE entitled "Cloud infrastructure services: an analysis of potentially anti-competitive practices", October 2021.

[313] BYOL is a licensing model that allows them to be used both on-premise and in the cloud.

deployment options[314]. According to press reports[315], some complainants and Microsoft are therefore exploring a negotiated solution to the issues raised in the original complaint. However, this case was still ongoing at the time of publication of this notice.

484. Another example of restrictions concerns certain Oracle products. This cloud service provider is a long-standing player in the on-premise software market, whose licensed products, such as databases, are widely known and used by developers around the world. Oracle now offers its database services in the cloud, as PaaS or SaaS software.

485. Some of these services are licensed and customers can choose to import them into a non-Oracle cloud environment[316].

486. However, Oracle database licences can only be imported into third-party cloud environments approved by Oracle, *i.e.* to date, AWS and Microsoft Azure[317]. For example, it is not possible to import Oracle licences on Google Compute Engine (GCE) machines.

487. In addition, through pricing or trade practices, certain software licences required for the provision of specific cloud services are becoming excessively onerous for the customer provider, which is no longer able to source them from its software publisher. One cloud

[314] Microsoft's announcements for 1 October 2022 were as follows:

- customers will be able to receive extended rights of use on Microsoft software held on-premise, enabling them to run their software, including Windows 11, on the servers of multi-tenant hosting providers, and more easily obtain virtual machine licences for Windows Server;
- Windows Server will be licensed on the basis of a virtual kernel, whereas previously it was only licensed on the basis of a physical kernel, making it easier to license Windows Server for virtualisation or outsourcing. Cloud service providers other than Microsoft will therefore in theory be able to attract customers with Windows Server workloads in place by allowing them to move these workloads from on-premise servers to the cloud;
- Microsoft will make it easier to virtualise Windows 10 or Windows 11 by removing the Virtual Desktop Application (VDA) add-on licence requirement for Microsoft 365 F3, Microsoft 365 E3 and Microsoft 365 E5 users who want to virtualise Windows 10 or Windows 11 on servers and do not have a primary Windows Pro device;
- as part of the new flexible virtualisation benefit, customers will be able to work with partners in the Cloud Solution Provider programme to obtain pre-built hosted desktop and server solutions, and either bring their own licence or license it from the partner. A Microsoft customer contract with the participating partner and proof of a licence will be required to run these hosted solutions;
- customers will be able to choose between one- and three-year subscriptions for a wide range of products, including Windows Server, Remote Desktop Services (RDS) and SQL Server, through Cloud Solution Provider partners, offering price stability with long-term subscriptions.

[315] See, for example, the article *"Microsoft reportedly convinced OVHcloud to withdraw its complaint"*, 31 March 2023 (link). CISPE is critical of Microsoft's proposals (see, for example, CISPE press release, "*Agent Smith and The Microsoft Matrix - Or how Microsoft spent the past 12 months convincing us that the Azure pill is the best choice*", 31 May 2023, link).

[316] In this respect, one hyperscaler stated that its customers can *"use an Oracle database engine on its environment on the basis of two licensing models: a "licence-included" model, in which the customer can obtain the database engine licence through" the provider, and a "bring your own licence" model, in which the customer obtains the database engine licence from Oracle and operates the database on the provider's environment".*

[317] See also the list of authorised vendors under this link. These approvals define the rules for counting Oracle CPUs (the unit of measurement used to determine the number of Oracle licences a user must subscribe to), and therefore the number of licences required by the cloud service provider's customers.

service provider pointed out that Oracle's database services are not easy to use in the cloud, stating that "*to provide an Oracle licence for a VM* [virtual machine] *core in the cloud,* [it] *would have to license all the processors in its cloud, on a per-customer basis. This would mean extremely high costs for* [the provider] *and for the customer, who would be unable to accept this type of offer*". The investigation showed that several providers are facing the same problem.

488. Other Oracle-licensed products simply cannot be used outside the Oracle cloud environment. This is the case, for example, with the product known as "Oracle RAC" (Oracle Real Application Clusters), whose terms of use clearly state that "*Oracle does not support Oracle RAC on non-Oracle public cloud environments*" [318].[319] However, one hyperscaler pointed out that "*Oracle RAC is a single product that is widely implemented in companies and leverages this advantage by preventing its customers from running Oracle RAC on any other cloud*".

489. In addition, some companies in the software sector apply a waiting period before their licence can be reused in another environment, resulting in additional costs when switching a workload from one environment to another, since two licences are required for the duration of the migration.

490. Furthermore, some software vendors restrict cloud service providers' access to their software, even though it is essential for the provision of certain cloud services. These are pricing restrictions, for example when it is less expensive for a customer to purchase this software directly from the publisher. For example, Microsoft has set up the "*Azure Hybrid Benefit*" [320] mechanism, which provides customers with a financial incentive to stay with its environment.

491. Another highlighted practice is the use of audit strategies with software users to verify their compliance with the publisher's policy. Faced with the risk of non-compliance, many customers would like to regularise their situation through commitments to purchase cloud services.

492. Alongside the practice of getting their incumbent on-premise software customers to use their cloud services, some providers link the two services through tied selling and pricing advantages.

Tied selling practices and price advantages

493. The investigation showed that cloud service providers may use certain exclusivity practices or targeted pricing practices to restrict customers' ability to use other providers.

494. In particular, several customers reported that, as part of their migration to the cloud, they were forced to accept new proprietary products and services systematically associated with cloud services. These practices would prevent customers from combining the cloud services they want from their historical software publisher with other services that could have been offered by third-party providers. Other customers have experienced technical or pricing

[318] See Oracle's document on implementing Oracle RAC on third-party clouds (link and link).

[319] Oracle RAC is an option for Oracle database software produced by Oracle. It allows customers to run a single Oracle database on multiple servers to optimise availability and enable horizontal scalability, while accessing shared storage (see Oracle website).

[320] Economic advantage offered by Microsoft, presented online (link).

difficulties in using services other than those of their incumbent software publisher for the same workload when migrating to the cloud.

495. In addition, several customers indicated that promotional operations or specific pricing models may have been put in place to encourage on-premise software customers to switch to cloud services. As mentioned above, cloud credits may also have been offered to some on-premise software customers, with the provider granting them credits that can only be used on its cloud (linked cloud credits). Other customers criticised the fact that obtaining advantageous pricing conditions on on-premise software depends on subscribing to cloud services.

496. During the investigation, several players also reported significant price increases on certain SaaS products, when bundled with cloud solutions. They stated that the move to a SaaS model is instrumental in changing the trade relationship, as the shift from a perpetual licence system to a subscription model increases the difficulty of renegotiating contracts and therefore leads to higher overall costs. Customers are then faced with a major change in pricing, as they move from a one-off licence purchase (with regular but optional paid updates) to a pay-as-you-go pricing model (in the form of monthly subscriptions, for example) for cloud services. In addition, the integration and bundled pricing of a SaaS offering with a simultaneous IaaS/PaaS service can reduce the ability to analyse the real cost of the solution.

497. In general, many customers complained that some software vendors are no longer willing to provide their software on-premise, and are forcing the switch to cloud mode. Stakeholders agreed that the move from an on-premise to a cloud model is likely to reinforce customers' dependence on their software publisher. This is because, in the event of a breakdown in trade relations, unlike the on-premise model, where customers retain ownership of their licence, in a cloud model they can no longer use the cloud software they have subscribed to. The technical integration of the software with the cloud solution also makes it more expensive to migrate to other software.

498. As one cloud service provider summed up: "*Software vendors with significant market power are able to use this market power to develop their presence in the cloud, offering more favourable conditions to users who migrate to their own cloud rather than to that of their competitors. This is the case, for example, when a software publisher allows its customers to continue using their "classic" user licence when they migrate to the publisher's cloud, but requires the purchase of a separate licence when they migrate to a third-party cloud*".

Technical restrictions

499. In addition to commercial and pricing restrictions, some providers also use their privileged position in related software solution markets to undermine the quality of the solutions offered by their competitors and promote their own solutions. These obstacles could consist of "*limiting usage rights to 'off-premise'* [and] *making available fewer security feature updates, usage flexibility and technical support*" compared to what is available with their own programmes.

Specific competitive risks

The *Autorité* has identified specific competitive risks in three different scenarios, depending on whether we are looking at the situation of customers when they first migrate, i.e. migrating on-premise information systems to the cloud, or when migrating from one cloud service provider to another. The last scenario concerns barriers to expansion for hyperscalers' competitors.

Specific competitive risks associated with first-time migration

Migrating customers from on-premise solutions to the cloud is complex and costly. This can lead them to turn to their incumbent IT service providers that are also cloud service providers, when it comes to choosing their cloud services.

The investigation uncovered practices likely to reinforce the disincentives for a customer to use an alternative cloud service 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 are currently before the European Commission on the basis of similar practices.

2. SPECIFIC COMPETITIVE RISKS ASSOCIATED WITH MIGRATING FROM ONE CLOUD SERVICES PROVIDER TO ANOTHER

500. Impediments to migrating to another provider for cloud-hosted workloads can undermine the functioning of competition, preventing customers from switching cloud service providers if their current provider's services no longer suit them, or if the services of an alternative provider are more attractive.

501. The investigation revealed that there are significant risks of customer lock-in, at least in terms of workload, (see Part II) in the cloud sector. 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[321], it is already apparent that migration from one cloud service provider to another can be hindered by technical barriers, as well as by deliberate practices by providers.

a) Technical barriers associated with a migration from one cloud service provider to another

502. Technical barriers to migration can appear at various levels, linked to the specific architecture and solutions used. In particular, 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.

Provider-specific services

503. As seen earlier, most cloud service providers offer their own proprietary services, or services tailored to their own technological choices. The variety of offerings from cloud service providers can slow down the implementation of migration to an alternative cloud service. For cloud technologies, some services, especially among the most widely marketed, particularly at the infrastructure level, seem to be undergoing a form of standardisation. However, there are still substantial differences between the infrastructure services (IaaS) of the various providers. This observation seems even more true for the most recent and innovative services, especially for PaaS.

[321] Almost 61% of the customers who responded to the Autorité's questionnaire have not switched or attempted to switch to another IaaS cloud service provider. The percentage is nearly the same for a change in PaaS cloud service provider) almost 57% of the customers who responded to the Autorité's questionnaire have not switched or attempted to switch to another provider).

IaaS services still partly differentiated

504. In terms of infrastructure, basic services such as storage, networking and computing are the most standardised cloud services. Several players in the sector refer to this as a "*commodity*". These services are provided in a similar way by all cloud service providers, although there may be variations in terms of invoicing or service guarantees. As a result, customers who limit their use of cloud services to infrastructure services can, in theory, easily move workloads (usually in the form of virtual machines) from one cloud environment to another.

505. Nevertheless, stakeholders cited several technical obstacles to migrating applications from one IaaS provider to another:

- the architecture implemented by customers: customers may have added extra layers to a cloud infrastructure for security, networking or DevOps[322] purposes, for example, or when the characteristics of certain provider networks require it, such as the ability to ingest large volumes of data. Machine versions and types can also hinder the "as-is" migration of legacy environments. In practice, this means, for example, that an IaaS configuration on Microsoft Azure dating back to 2017 may be complicated to migrate to another cloud service provider, as machines, operating system versions, software layers and even security patches will have evolved and the whole architecture will need to be rethought. Lastly, the issue of compatibility between the licensing models offered by the IaaS host and the software vendors is also cited as an obstacle (for example, if the software is implemented on an operating system that is not offered by the IaaS host);
- dependence on infrastructure as code: the main technical obstacle identified is dependence on the "code languages" specific to each cloud service provider, even if today open-source tools such as Terraform considerably (but not totally) reduce compatibility and portability problems. One provider also pointed to the lack of standardisation in application programming interfaces[323], which means that "*you have to adapt your code to the cloud provider*";
- contractual provisions: these may not clearly define the technical specifications of IaaS services, particularly in terms of networks.

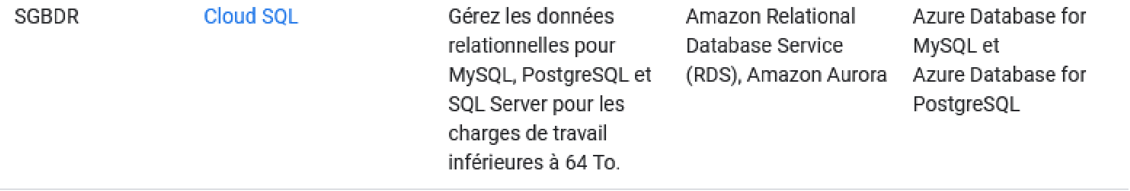
PaaS services often provider-specific

506. As seen earlier (see Part II), providers are seeking to differentiate themselves by offering innovative, value-added services, particularly in PaaS. Proprietary technologies are particularly plentiful in the higher layers (big data, artificial intelligence, collaboration tools, database management systems, authentication layers, identity repositories, etc.). As a result, not all products and services offered by cloud providers necessarily have an equivalent with another provider, which limits the possibility of using different providers. One product can therefore correspond to several equivalent products from other providers. By way of illustration, a Google Cloud database product such as Google Cloud SQL can correspond to several products at Amazon and Microsoft, as shown in the example below.

[322] See glossary.

[323] See glossary.

Figure 21 - Match between a Google Cloud service and another provider



SGBDR	Cloud SQL	Gérez les données relationnelles pour MySQL, PostgreSQL et SQL Server pour les charges de travail inférieures à 64 To.	Amazon Relational Database Service (RDS), Amazon Aurora	Azure Database for MySQL et Azure Database for PostgreSQL

Source: Extract from the Google Cloud website[324]

507. As a result, the process of migrating a workload based on one or more proprietary PaaS services is made more complex by the need to fundamentally modify the way the workload functions, so that it works without these specific services. One hyperscaler pointed out that "*if a customer creates an application that they run in the cloud and that depends on a proprietary PaaS service from a particular cloud provider, they will not be able to move that application entirely to another cloud without first resolving that dependency.* [...] *The cost and duration of this rewrite will depend on the complexity of the application and how it is used. In any case, this will require more effort than moving an agnostic virtual machine to the cloud. And, of course, the more integration points with proprietary services a customer has, the more work it will take to replace them*".

508. According to some hyperscalers, these barriers should be put into perspective, as some proprietary services are based on open-source solutions. One hyperscaler explained that "*many proprietary cloud-specific services are based on open-source solutions, and versions of these solutions are available on every public cloud, whether offered as a first-party service (e.g. Azure Kubernetes Service, Google Kubernetes Engine, Amazon Elastic Kubernetes Service) or as a third-party service (Red Hat OpenShift, Docker Enterprise, Rancher Kubernetes Service, etc.). And even for cloud-specific services not based on open source, public clouds generally offer similar proprietary services to compete with each other (for example, AWS, GCP and Azure all have translation and text-to-speech APIs).*" However, proprietary services based on open-source solutions do not appear to be in the majority in provider catalogues. For example, of the 300 cloud services presented by Azure[325], around 10%[326] are based on open-source solutions.

Complex migration operations

509. When a company wants to migrate to a new cloud service provider, it will have to carry out complex, time-consuming and resource-intensive operations, such as readapting existing code for a lift-and-shift migration or rewriting the entire code for a total refactor.

510. The lack of portability of applications[327] or data[328] can be a major difficulty in migration projects. To ensure the portability of certain applications (or workloads), for example, the company must change all its connections to the original provider's application programming

[324] https://cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison?hl=en.

[325] https://azure.microsoft.com/en-us/products/.

[326] Estimate based on the investigation.

[327] Application portability refers to the ability to migrate applications from one provider to another.

[328] Data portability involves the originating cloud service provider making the raw data and its schema available for re-integration into the destination provider's database engine.

interfaces to the services of the destination provider. One of the main problems with the portability of applications is that data lakes[329] are difficult and costly to move. They therefore act as "*centres of gravity*"[330]. Data portability is also made more difficult if data is stored in proprietary databases whose re-use would require considerable transcription work. A study carried out for the Commission in 2018[331] confirmed that low levels of data format parity between providers are a significant and complex barrier to switching providers.

511. Differences in design and use may require the creation of a new architecture or the modification of source code, with a potential impact on the service provided. Some providers do not offer certain types of software, operating system or database management system licences, which prevents or complicates the migration of certain applications developed on these types of licences. According to one customer, "*the main obstacles are the cloud services using non-standard APIs, which means rewriting part of the application code*". Ultimately, for one cloud player, "*by offering more automation and industrialisation, PaaS also presents more barriers to entry and exit*".

512. Some technological solutions, such as container technology, aim to facilitate migration processes. One cloud service provider confirmed: "[We] *offer public cloud solutions based on open-source technologies such as OpenStack (a platform that controls diverse, multi-vendor pools of processing, storage and networking resources) and Kubernetes (an industry-standard container orchestration platform). Using these standard platforms offers customers easy data transfer capability and access to source code, facilitating reversibility and eliminating 'provider lock-in*'". From the customer's point of view, technology such as Kubernetes, which has become a market standard, is in high demand as it makes it easier to migrate from one provider to another.

513. Nevertheless, one cloud service provider qualified that: "*for a product such as Kubernetes (container orchestration), which can be considered a market standard today, the issue is more complex. Interoperability is relatively good, but portability less so, as migration requires rewriting all or part of the application deployment documents. Each cloud provider has its own specific technical specifications (unique tools, ad-hoc methods, etc.) which would be difficult (if not impossible) to harmonise*". In addition, another provider considered that the service's impact on the cloud sector as a whole is limited for the time being, insofar as interoperability difficulties remain for the majority of hyperscalers' services: "*although Kubernetes is interoperable, since it is open source, it only represents a very marginal percentage of the market, and technical lock-in phenomena are occurring on the rest of the services offered by hyperscalers* [...]. *In addition, highlighting Kubernetes to illustrate supposed interoperability and ease of migration can be a red herring, in other words, a loss leader that ultimately contributes to locking users in*".

[329] See definition in part 1.

[330] Blog post on the Gartner website, Marco Meinardi, "*Why adopting Kubernetes for application portability is not a good idea*", 4 September 2020 (link).

[331] Study carried out for the European Commission by IDC and Arthur's Legal: "*Switching of Cloud Service Providers*", 8 May 2018, page 29. According to this study, "*Data portability is the ability to easily transfer data from one cloud service provider to another cloud service provider without being required to export and re-import the data; similarly, application portability is the ability to easily transfer an application or application components from one cloud service to a comparable cloud service and run the application in the target cloud service*" (link).

b) Technical and commercial practices likely to contribute to customer lock-in

514. In addition to the disincentives associated with the technical characteristics of the services, providers can voluntarily put in place additional technical and commercial barriers that can contribute to customer lock-in.

515. From the technical standpoint, practices aimed at integrating all the services and solutions could have anticompetitive effects (or even an anticompetitive purpose if the practices aim to close the system) if implemented by a company in a dominant position.

516. In a similar way to the technical restrictions likely to be implemented for a primary migration to the cloud (see Part IV. B. 1 b), several stakeholders confirmed the existence of technical restrictions on the use of previously acquired software that may limit or prevent customers' ability to change provider. A report published for CISPE also noted that: "*software providers may employ operating specificities or proprietary language to reduce the ease of interaction (and eventually migration) between systems*"[332]. The report also pointed out that software providers can also capitalise on customer concerns regarding potential compatibility issues as a way of keeping users on the native platform.

517. Other technical restrictions are possible, such as deliberately using a specific data format to prevent the portability of a customer's data to an alternative cloud service provider.

518. Providers may also be able to impose commercial conditions that contribute to locking customers into their ecosystem.

519. As seen above, given the imbalance in the relationship between cloud service providers and their customers, providers may be able to impose trade conditions that contribute to locking customers into their ecosystem. Confronted with the difficulty of negotiating their contracts and a complex, unclear contractual architecture, customers could be led to accept clauses that limit their ability to migrate. Depending on the duration of the contract and the terms of its termination, these clauses could be problematic, leading to a lock-in of customers.

520. In addition, providers can also increase migration costs through their pricing structure. As seen earlier, the egress fees charged by hyperscalers, which are difficult to predict during the initial migration to the cloud, represent significant transfer costs and a substantial barrier to market contestability for subsequent migrations by hyperscaler customers.

Specific competitive risks associated with a migration from one cloud service provider to another

Impediments to migrating to another provider for cloud-hosted workloads can undermine the functioning of competition, preventing customers from switching cloud service providers if their current provider's services no longer suit them, or if the services of an alternative provider are more attractive.

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. In particular, 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

[332] Mr Frédéric Jenny, "*Cloud Infrastructure Services: An analysis of potentially anti-competitive practices*", October 2021, page 44.

significant migration costs. In addition to the technical obstacles, providers 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 service provider. Providers may also be able to impose commercial conditions that contribute to locking customers into their ecosystem.

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

521. The imbalance in relations between certain providers and their customers, as described above (see Part IV.A), may have the effect of dissuading their customers from using alternative cloud service providers in parallel, for the performance of certain services. On the other hand, from a technical point of view, obstacles to interoperability can create barriers to expansion for hyperscalers' competitors. Certain practices could also reinforce these obstacles to multi-cloud.

522. However, interoperability is beneficial to competition, since it enables rival providers to receive the same leverage effects as dominant providers while competing with them in areas that are important to customers (such as price or quality of service).[333] The stakes are particularly high for providers other than hyperscalers, as the survey showed that hyperscalers enjoy a number of advantages when the choice of their first cloud service provider is made, and that there are numerous obstacles in the way of migration from one cloud service provider to another. It should also be noted, however, that forced interoperability on innovative products may reduce the incentives to innovate, as the profits from innovation may then be shared with third parties.

a) Technical obstacles to multi-cloud

523. The industry is plagued by technical obstacles to interoperability and multi-homing. Although these practices affect all competitors, they have a greater effect on smaller providers, given the attractiveness of cloud ecosystems when it comes to choosing a new provider (see Part II).

524. As seen above, hyperscalers provide a service integrating a set of underlying services managed in-house and working closely with their other services. This integration can create technical obstacles for customers wanting to use different solutions provided by other operators. It can also be difficult to associate an external product with the existing cloud service provider's architecture, especially when it is based on proprietary standards. According to one cloud service provider, the integration of a provider's services is a major obstacle to multi-cloud, because "*it is always easier to use automation tools to move data from one process to another within the same provider, rather than having to export this data in a standard format so that it can be reused by another provider*".

525. Below are a few examples of the practical consequences of the limited interoperability of IaaS and PaaS services, to the detriment of other providers (see boxes below).

[333] Yale Tobin Center for Economic Policy, K. Seim, "*Equitable Interoperability: the "Super Tool" of Digital Platform Governance*", 13 July 2021.

Amazon's standard "S3" service

Amazon Simple Storage Service (Amazon "S3") is an object storage service that offers industry-leading scalability, data availability, security and performance. This protocol has become the *de facto* standard for object storage in the cloud, so much so that all cloud service providers now offer a "compatible" object storage service, i.e. one that follows the same syntax and operation as the Amazon "S3" application programming interface, to achieve the same level of service as the AWS implementation. In practice, AWS continues to maintain this standard, evolving it over time to meet new use cases and changing needs.

In view of the ongoing development of this service, AWS provides third parties (especially developers) with detailed public documentation and access to its API (for third parties who pay for this service) so that they can ensure that their solutions are compatible with "S3". It is in AWS' interest to make this information public, so that its adoption by developers is as widespread as possible.

However, despite this public nature, third-party cloud service providers report difficulties in implementing interoperability in practice.

One cloud service provider pointed out that unilateral modifications by AWS are regular and sometimes substantial, resulting in significant operating costs to ensure at the very least compatibility and, if possible, interoperability and data transferability in the environment of third-party providers. As a result, there is a mismatch between the "S3" service offered by AWS and the compatible services offered by third-party providers. However, if "S3"-compatible services are not fully interoperable with the standard, customers will be encouraged to use the AWS service directly.

526. The technical obstacles to interoperability can be even greater for a database PaaS service, for example.

Interoperability with PaaS services

For example, a company might have developed an application using cloud services from the original provider. To meet its needs, it will have used several services from this provider: virtual machines, storage (IaaS), as well as database management and *machine learning* services (PaaS). Part of the application code is therefore dedicated to these connections to the different services required. For example, connections to the database service's application programming interface are used to create databases, run queries, and so on.

If the company plans to change cloud service providers for the database service, it must be able to connect its storage at the outgoing provider with the database service of the incoming provider. Other PaaS services must also be able to communicate.

At present, this operation is difficult, not least due to syntax issues, as changing the PaaS database service also requires rewriting the part of the application code that uses that service.

In concrete terms, to create a database via the command console, different commands must be used for each provider. For example, on Cloud SQL (Google Cloud) it is essential to use the command: "***gcloud sql databases create***", while on Azure SQL (Azure): "***az sql db create***", and "***create-db-instances***" on AWS RDS (Amazon). At first glance, these changes do not appear difficult to implement. However, these commands potentially have to be repeated thousands of times in the application, making the process time-consuming and costly. These different commands also have different parameters, making it difficult to adapt and switch from one to the other. Furthermore, there is no centralised source for the different documentation, which has to be compared manually by the developers to identify the equivalent commands in the destination provider to those used by the originating provider.

Another difficulty is related to proprietary standards for certain services. According to one cloud service provider, "*most of the databases distributed globally by the GAFAM are totally proprietary (Bigtable for Google, DynamoDB for AWS, Table Storage for Azure*".

Lastly, others pointed to the lack of standards for PaaS services, given the dependence of these services on the platform provided by the original cloud service provider.

527. The consequence of this lack of interoperability is that some players (e.g. Google with its Big Query Omni service) are developing "intermediate overlays" that make it easier to connect the services of different providers and resolve certain syntax problems, for example. However, some providers, notably hyperscalers, believe that it is not possible to impose total interoperability between cloud services. One explained "[that] *it is difficult to enable full interoperability between services; for example, full interoperability of new services with pre-existing services or protocols may be technically impossible and, even if it is possible, may create a security risk (e.g. certain older cryptographic protocols for secure communication) or significantly delay the availability of the service to customers. In addition, there are services* [...] *that are only available on* [...] *because the underlying technology is a* [...] *unique innovation*". The difficulty of ensuring interoperability between specific services was confirmed by some providers that are not hyperscalers. For example, managing user identities and access would be very difficult, as "*management is different from one cloud provider to another, and* [...] *interoperability is not guaranteed or even possible*". It is clear from the above that the more varied and sophisticated the services a customer uses, and the more they are based on proprietary standards, the more difficult it will be to ensure interoperability with an alternative provider.

528. In terms of multi-homing (see Part I. B. 4), this could be justified, for example, for workloads requiring a very high level of availability (as in the financial sector), to compensate for possible provider failures. This possibility would appear to be a factor in favour of competition, limiting barriers to entry and expansion, enabling a better comparison of offers and reducing the risk of dependence on a single provider. However, the investigations showed that, on the customer side, multi-homing strategies are underdeveloped, mainly due to voluntary practices by certain providers. In particular, one cloud service provider reported that "*anticompetitive licensing practices, technical restrictions (such as proprietary APIs and complex licences), data protection and cybersecurity compliance issues, and high costs, are the main obstacles to multi-homing*".

529. Providers, especially dominant ones, may actively seek to leverage these technical barriers to interoperability or adopt behaviours designed to amplify them, in order to exclude their competitors from the market.

b) Practices linked to a provider's presence in several related markets:

530. Certain practices could contribute to increasing the disincentives to multi-cloud, and therefore be likely to have an impact on the competitive functioning of the sector.

Restricting competitors' access to the software needed to provide cloud services

531. The relationship between a software publisher, who is also active in cloud provision markets, and another cloud service provider (see above) can give rise to competitive risks. As the provision of certain cloud services requires the use of licences from software vendors, a

provider may be both a customer of a publisher for the provision of licences, and in a competitive situation with the same company for the provision of cloud services.

532. As indicated above, the investigation revealed that, through pricing or trade practices, certain software licences required for the provision of specific cloud services are becoming excessively onerous for the customer provider, which is no longer able to source them from its software publisher (see Part IV). B. 1). In this way, a software publisher in a dominant position can leverage its position to drive out some of the competition and win customers for its cloud services.

More advantageous commercial or technical conditions for the provider's own products or services

533. Similar to the practices seen when customers migrate to the cloud (see above), larger cloud service providers may resort to tied selling practices, price advantages or technical restrictions to limit the expansion of third-party providers.

534. The investigation revealed that cloud services can be included in bundles of several digital products and services. On this point, several customers indicated that this is a frequent practice that can lead to the purchase of services that do not meet their requirements. Bundled offers can also make it more advantageous to buy from a single, integrated provider for all needs.

535. In a 2020 report, the Antitrust Subcommittee of the U.S. House of Representatives had already noted the anticompetitive risks of Google's strategy: "*Google's documents suggest the company is considering bundling its popular machine learning service with other services that Google is seeking to promote. A recent document on Google's cloud pricing strategy explains that "One recent Google cloud pricing strategy document explains, ''the question that we need to think about is whether we use our entry point with Big Query to get a customer to use all the services such as Data Proc, Data Flow, as a suite and give them a price break on the Analytics Suite because it will be much harder for them to migrate away from us if they use all the other services". The document goes on to describe potential discounts and ultimately a plan to have ''a pricing model that makes it advantageous for customers to put 80 percent of their workload on GCP"*[334].

536. Furthermore, a player with market power in related markets can also use this power to promote the development of its cloud activities and distort competition on the merits. Due to their conglomerate structure, hyperscalers can develop discount systems, tariff and non-tariff benefits or cross-subsidies, making it easier to develop their cloud business due to their other activities. According to one provider, a well-established player, for example, in the advertising or online collaborative working tools market, could offer significant discounts on its cloud offerings to the largest users to encourage them to migrate to its own cloud offering to the detriment of competitors.

537. This type of practice could therefore form part of an overall strategy aimed at leveraging market power in a related market to pre-empt cloud markets. In its aforementioned report, the Antitrust Subcommittee of the U.S. House of Representatives made this observation: "*Google appears to leverage its dominant business lines, including popular APIs such as Google Search and Maps, along with machine learning services, to attract customers to its platform through discounts and free tier services. For example, according to internal*

[334] US House of Representatives Sub-Committee on Antitrust, Investigation of competition in digital markets, 2020, p. 269 (link).

strategy documents, in 2018, Google "launched a program with the Play team to provide GCP credits to game developers based on their Play Store spend, to increase focus on Play and incentivize migration to GCP." By harnessing Google's advantages in existing markets, GCP is undermining competition on the merits"[335].

538. The conditions under which cloud credits are granted (see Part I.D and Part IV.A) could also reward group purchases of cloud and non-cloud services. This point is contested by one hyperscaler, for whom cloud credits do not constitute a tied selling practice, in the sense that they are not linked to the sale of non-cloud products from its catalogue. However, one rival provider argued the opposite during the public consultation: "*By tying cloud services to non-cloud solutions (such as software), dominant operators are aiming to oust their competitors*". This type of practice can form part of an overall strategy linked to leverage capabilities (see c below). In addition, some stakeholders consider that there is a risk of leverage between the dominance of hyperscalers in related markets and their ability to enter the cloud market through cloud credits. For example, in its recent ruling in the "Google related rights" case, the Paris Court of Appeal noted that: "[Google] *points out that certain agreements entered into by Google may combine different products or services (for example, an agreement on advertising may also include cloud credits)* [...][336]".

539. Lastly, customers of competing providers could be subject to technical restrictions that could impact the availability, functionality or security of these services. Other restrictions could involve deliberately lowering the quality of certain solutions in cases where they are operated by another player. Some stakeholders confirmed the existence of such practices within the sector.

Imbalances in data access that may favour providers with a conglomerate structure

540. As seen earlier, their conglomerate structure can enable hyperscalers to enjoy advantages linked to data collection in different markets. The investigation for this opinion highlighted several risks in this respect.

541. First, 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. Through better sales targeting and a more detailed understanding of customer needs, this analysis can improve existing service functionalities and develop new tools, such as artificial intelligence or machine learning. These developments can have a positive impact on consumers and innovation. But 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. According to one provider, "*the asymmetry of data access currently observed on the market severely limits the scope for competing operators to develop innovative and competitive solutions*".

542. Furthermore, some customers reported competitive risks associated with the use of their data, when their cloud service provider is also - via another subsidiary in particular - a

[335] US House of Representatives Sub-Committee on Antitrust, Investigation of competition in digital markets, 2020, p. 26 (link).

[336] See the Paris Court of Appeal (Cour d'appel de Paris) ruling under this link.

competitor in another market. This would give hyperscalers access to strategic data that they could exploit to strengthen their market position. Some companies are therefore concerned about their lack of visibility over their cloud service provider's use of their internal data.

543. All these behaviours, which enable providers to use their market power in a related market, contribute to a conglomerate dynamic, with knock-on effects that enable the operators concerned to strengthen their position in all their markets, to the detriment of more specialised players. This dynamic can reduce the choice for users and weaken the development of alternative solutions.

c) Other practices

Risks associated with cloud credits and egress fees

544. As seen above (see A.2), cloud credits are likely to form part of strategies that limit the expansion of competitors, since they would have the effect of preventing smaller competitors from replicating cloud credit offers equivalent to those proposed by hyperscalers. In addition, the use of multi-cloud is likely to be limited by high and unpredictable egress fees (see A.2 above).

Risks relating to the conditions of access and use of cloud marketplaces by third-party providers

545. As seen above (see Part II.C), some cloud service providers offer marketplaces that allow third-party publishers to offer complementary products or services to their customers. These marketplaces are a way for a provider to enhance its cloud ecosystem, but can also be used to control the conditions of access and operation of the third-party solutions within it. As such, marketplaces can be a way for providers to limit the ability of third parties to compete with them, and thus have an impact on competitive dynamics.

546. Marketplaces are just one way for publishers to market their services, as they have multiple distribution channels at their disposal. They can generally market their services directly, *via* intermediaries, and practise multi-homing on different platforms. In particular, one hyperscaler considered that contracts are frequently concluded outside its marketplace, even if one of its customers may have discovered the service *via* the marketplace. Overall, according to one cloud service provider, marketplaces currently only play a secondary role in the marketing of cloud services and are therefore unlikely to be conducive to lock-in or discrimination effects.

547. This finding echoes those of the ACM in its study published in September 2022: "*The requests for information that ACM sent to providers show that in terms of revenues the marketplace plays a relatively small role at present. Interpreting the role of the marketplace solely on the basis of revenues seems too short-sighted, however. Some services are provided free in the marketplace and it is possible that third-party services can be found through marketplaces of the major providers, but that these third parties are then approached directly. The discussions conducted by ACM revealed that third-party services are widely used, but that relatively few are purchased through the marketplace*"[337].

548. While the role of marketplaces is currently still minor (see Part II.C), the information collected during the investigation nevertheless suggested that they are tending to grow in

[337] ACM Market Study Cloud Services, published on 5 September 2022, page 41 (link).

importance, both for the providers of these platforms and for the publishers who offer their services on them.

549. For providers, the marketplace makes their ecosystem more attractive. Several players indicated that these marketplaces enable them to offer more services for a greater number of use cases. Providers' main strategy would be to provide attractive access conditions to attract developers of interoperable solutions. From this point of view, the use of the services offered on its marketplace can be seen by the cloud service provider as an enhancement of its offering, a factor in the development of its own business. According to one customer, the third-party products or services it purchased on the marketplace would be taken into account in the volume commitment with its cloud service provider in return for a discount. In certain limited circumstances (such as a volume commitment), these purchases of third-party services *via* the marketplace would therefore also benefit from the discount negotiated with the provider.

550. In view of the growth in the number of marketplaces, and the fact that some could become essential for third-party publishers, the *Autorité* considers that a number of competitive risks could emerge, particularly in relation to the conditions for accessing and operating these marketplaces.

551. Through their marketplaces, cloud service providers have the power to set conditions for third-party service providers to access their ecosystem. These conditions usually include several restrictions, for example regarding the type of products that can be marketed, the region of availability, the technical tools and licences used, and the other marketing channels authorised or hosting at the provider's premises.

552. The investigation for this opinion established that several restrictions currently exist in the conditions of use of the main marketplaces. For example, several 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. There are also restrictions on the type of services that can be marketed and their technical characteristics. On the Google Cloud Marketplace, Google defines a restrictive list of PaaS product types that can be sold and requires that Kubernetes applications and virtual machine products do not use Terraform[338]. Furthermore, marketplace providers generally have a great deal of power to intervene in their marketplace, not only to authorise access to third parties but also to exclude them for more or less explicit reasons.

553. It may be legitimate to impose certain conditions in the customer's interest on third-party publishers who have access to the marketplace (security, quality of technical integration, consistency of offering, protection of intellectual property, protection against parasitism, etc.). However, some can also make access unfair between players, and erect barriers to entry or expansion for new players. Through the marketplace, the provider can also promote its own solutions, in terms of both marketing and customer promotion, to the detriment of other services offered by third parties. These risks have to be taken into account and call for vigilance.

[338] Open-source tool that makes it possible to describe an infrastructure declaratively ("infrastructure as code"), independently of the (cloud or other) system in which it operates.

554. As part of its report on trade practices in the cloud services sector, the Japan Fair Trade Commission also looked at the pricing parity clauses[339] that providers can impose.[340] 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 the other marketing channels used. Although these clauses are not very widespread, mainly due to the still limited role of marketplaces, the JFTC highlighted several potential risks associated with this type of clause. In particular, it revealed a risk of higher non-commission selling prices in marketing channels with a lower sales commission, and a reduction in the ability to differentiate, and therefore in competition, between distribution channels.

555. The *Autorité* agrees with this analysis. Although the investigation has not yet revealed the existence of any pricing parity clauses, vigilance will be required in the future, particularly if marketplaces take on a more important role.

556. Lastly, the *Autorité* considers that the commissions charged by marketplaces may in the future be indicators of the essential nature of certain marketplaces, or even of certain ecosystems, and the importance of network effects. If certain marketplaces were to become essential, this could lead to an increase in commissions, indicating a situation of imperfect competition or, if the conditions are met, an abuse of a dominant position through the setting of an unreasonably high price.

Voluntary obstacles to interoperability

557. Cloud service providers offering popular products or services could prevent or limit access to key information needed to ensure the interoperability of these products or services with those of their competitors (see Part IV.B). This practice could have the effect of restricting the compatibility of competing solutions, and hence their attractiveness to customers and therefore create barriers to entry or expansion for competitors.

558. Some stakeholders confirmed the existence of such practices. One cloud service provider competing with the hyperscalers pointed out that "*the lack of interoperability (whether fortuitous or caused by the hyperscalers) is the main obstacle to using several providers for the same workload*".

559. Several providers reported that changes to certain standard services (such as the AWS "S3" service mentioned above) are made unilaterally and without prior notice, forcing competing providers to adapt in a hurry. It would seem that these changes are generally reported by certain customers, and not by the providers in charge of these services. As a result, a hyperscaler is able to offer updated services without delay, unlike its competitors.

560. In addition, the control exercised by certain hyperscalers over standard services or technical solutions promoting interoperability also raises concerns. One cloud service provider pointed out that "*the fact that some of the most widely used standards can be controlled by a specific player presents additional risks.* [...] *the 'technical solutions' that promote interoperability* [...] *are controlled by Google and Amazon (with the exception of Kubernetes, now operated by the Cloud Native Computing Foundation) and therefore present a number of risks for third parties wanting to use them*".

[339] Clauses imposing conditions that are favourable or as favourable as those provided for in other distribution/marketing channels.

[340] Japan Fair Trade Commission, Report on Trade Practices in Cloud Services Sector, published on 28 June 2022 (link).

561. Several reports confirmed that hyperscalers are deliberately hindering interoperability. According to the ACM, hyperscalers may adopt closed standards for the software used by their services and deliberately deviate from open standards to limit interoperability with the services of other providers. As a result, users cannot use different services from other providers, which is an obstacle to multi-cloud usage.[341] OFCOM's interim report on the cloud also confirms the existence of practices by hyperscalers, notably AWS and Microsoft, which appear to limit the interoperability of some of their services by not openly sharing information such as application programming interfaces (which may be unavailable to third parties) and protocols, or by combining proprietary standards with open-source software and standards, making it more difficult to use third-party providers.[342]

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

The industry is plagued by technical obstacles, particularly in terms of interoperability. These practices affect all competitors, but they have a greater effect on smaller providers, given the attractiveness of cloud ecosystems when it comes to choosing a new 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 a PaaS database service also 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 provider's presence in several related markets:

- restrictions on competitors' access to the software needed to provide cloud services: since the provision of certain cloud services requires the use of licences from software vendors, a provider may be both a customer of a publisher for the provision of licences, and in a competitive situation with the same company for the provision of cloud services. This may lead a software publisher to implement practices designed to increase the licence fees required by its competitors, or to make the use of its software subject to cloud environments benefiting from its approval, which in turn is conditional on the customer cloud provider purchasing a large number of licences for its own needs. In this way, a software publisher in a dominant position can leverage its position to drive out some of the competition and win customers for its 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, making it easier to develop their cloud business due to their market power in related markets;
- 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, risks related to the possibility for a provider to implement trade and pricing practices:

[341] Above-mentioned ACM market study, page 61.

[342] OFCOM interim report on a market study of cloud services, 5 April 2023, page 183.

- the impossibility, especially for smaller providers, to replicate cloud credit offers identically;
- the impact of egress fees on multi-cloud strategies.

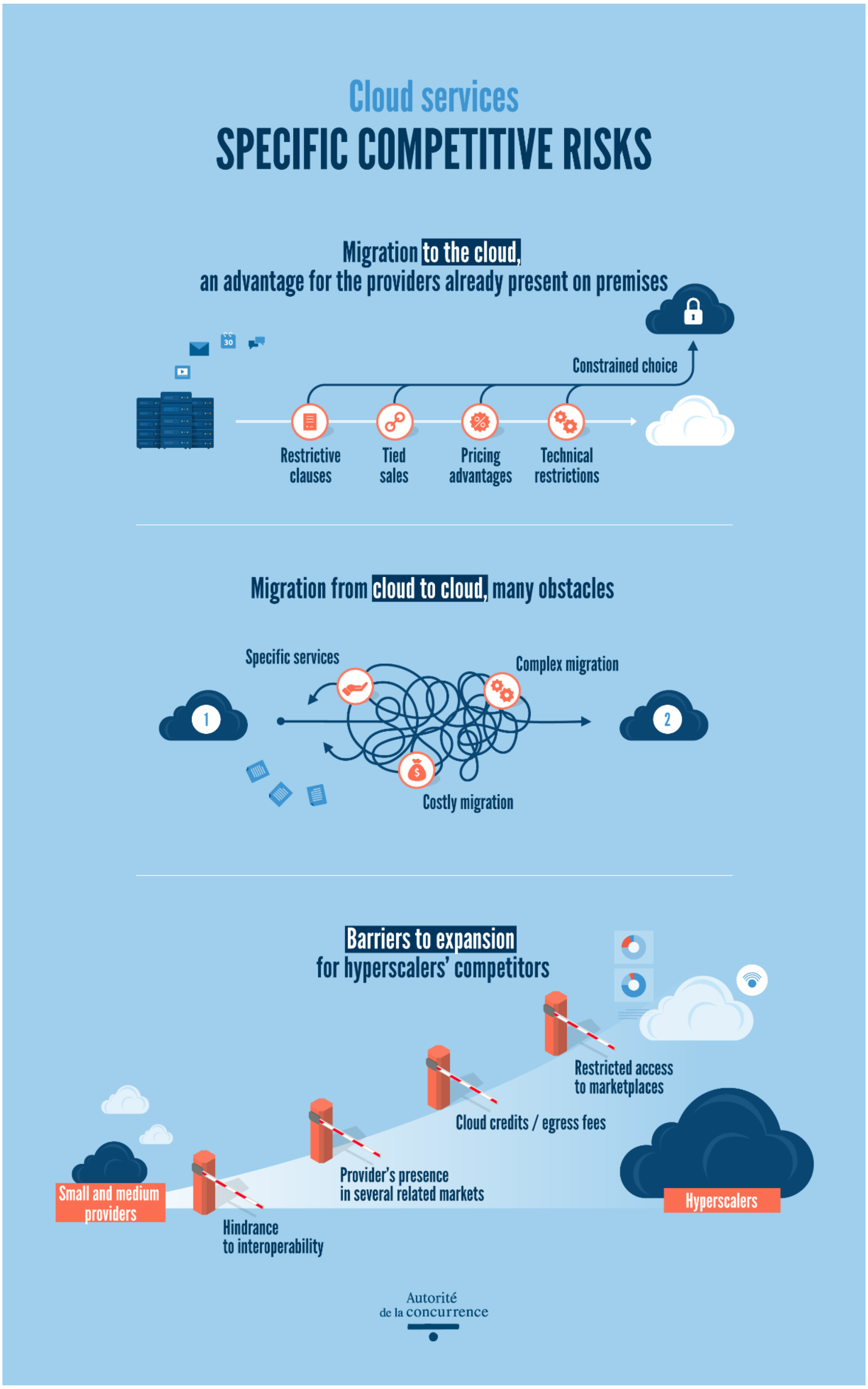
Thirdly, the *Autorité* also expresses a number of points of concern with regard to other practices.

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 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;
- lastly, 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 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 therefore have the effect of restricting the compatibility of competing solutions, and hence their attractiveness to customers.

Figure 22 - Specific competitive risks



Cloud services

SPECIFIC COMPETITIVE RISKS

Migration to the cloud,
an advantage for the providers already present on premises

Constrained choice

Restrictive clauses

Tied sales

Pricing advantages

Technical restrictions

Migration from cloud to cloud, many obstacles

Specific services

Complex migration

Costly migration

Barriers to expansion
for hyperscalers' competitors

Small and medium providers

Hindrance to interoperability

Provider's presence in several related markets

Cloud credits / egress fees

Restricted access to marketplaces

Hyperscalers

Autorité de la concurrence

Source: Autorité de la concurrence

V. Competition law responses

562. The examination of competitive risks identified, on the one hand, the technical impediments to competition inherent to the cloud sector, and on the other, the risks linked to practices that the operators themselves might implement.

563. When it can intervene quickly enough, competition law is a particularly effective tool for maintaining the competitive dynamics of the digital economy. It is a soft, comprehensive law that has demonstrated its ability to embrace new practices and adapt well-established solutions to new services. In order to meet the challenges posed by the cloud, consideration could be given to using other instruments of Book IV of the French Commercial Code (*Code de commerce*), such as the law on restrictive competitive practices (E), alongside the classic competition law tools of abuse of a dominant position (A), combating illegal cartels (B), merger control (C) and abuse of economic dependence (D).

564. However, a regulatory approach seems better suited to resolving market failures already identified and known, as European and national regulators have also begun to implement in recent months, particularly with the DMA (Data Act) currently under discussion, and the draft law to secure and regulate the digital space (see Part VI above).

A. ABUSE OF A DOMINANT POSITION

565. The concept of abuse of a dominant position makes it possible to deal effectively with abuses committed by certain players who hold a dominant or even ultra-dominant position in the digital sector. In this respect, the *Autorité* would like to draw attention to a number of important decisions that could serve as a benchmark for action in the cloud sector. The *Autorité* also intends to use all the tools at its disposal to improve the efficiency and speed of its action.

1. A RICH BODY OF DECISION-MAKING PRACTICE THAT CAN SERVE AS A REFERENCE FOR ACTION IN THE CLOUD SECTOR

566. Competition authorities, notably the *Autorité* and the Commission, already have long experience of cases involving abuse of a dominant position in digital markets.

567. The investigation showed that some vertically integrated operators may treat their own products or services more favourably than third parties. Under Article L. 420-2 of the French Commercial Code (*Code de commerce*), the abusive exploitation of a dominant position can take the form of "*discriminatory sales conditions*". Furthermore, Article 102 TFEU expressly states, among the examples of abusive practices liable to constitute an abuse of a dominant position, that of "*applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage*". For example, in the "Google Shopping" case[343], the abusive conduct consisted of the more favourable positioning and presentation of the results of Google's own product comparison service in its general results pages compared with the results of competing product comparators. The

[343] Judgment of the General Court of the European Union of 10 November 2021, Case T-612/17.

Commission considered that Google's self-preference practice constituted an abuse of a dominant position prohibited by Article 102 TFEU, a decision upheld in essence by the European Court of First Instance.

568. Tied selling[344] and bundling[345] practices have also been the subject of important decisions by competition authorities. In France, in a non-digital sector, it was on the basis of tied selling that the *Autorité*, in its 2014 Nespresso decision[346], made it possible for Nespresso coffee machines to be interoperable with its competitors' capsules. Nespresso, the main player in the machine and capsule market, was likely to tie the purchase of its capsules to that of its coffee machines, thereby foreclosing competing capsule manufacturers. In the course of the investigation, the *Autorité* identified a number of technical, legal and commercial practices that encouraged consumers to use only Nespresso brand capsules in Nespresso machines. From a technical point of view, the *Autorité* noted that several successive modifications to Nespresso machines had had the effect of making capsules from competing manufacturers incompatible with the new models. The *Autorité* therefore considered that these practices, which were aimed at foreclosing competing capsule manufacturers, were likely to constitute an abuse of a dominant position. In response to these competition concerns, Nespresso committed to providing information on technical modifications, making machine prototypes available and appointing a trusted third party.

569. Moreover, like other organisations[347], the *Autorité* anticipates a gradual rise in cases leading to the adoption of measures to guarantee data portability and interoperability.

570. While the Commission has already stated that there is no general obligation under competition law, even for dominant companies, to ensure interoperability[348] with competitors' products or services, competition authorities have been able to condemn a dominant company's refusal to provide interoperability information. Article L. 420-2 of the French Commercial Code (*Code de commerce*) stipulates that an abuse of a dominant position or an abuse of economic dependence may consist of a "refusal to sell". In Microsoft v Commission (2007)[349], the General Court of the European Union upheld the Commission's decision, which had found that Microsoft's refusal to disclose interoperability information constituted an abuse of a dominant position, and ordered Microsoft to disclose this information to any company wanting to develop and distribute operating systems for

[344] In its Guidelines on the priorities forthe application of Article 82 of the EC Treaty [Article 102 TFEU] to exclusionary conduct by dominant companies (2009/C 45/02), the Commission states: "*Tying' usually refers to situations where customers that purchase one product (the tying product) are required also to purchase another product from the dominant undertaking (the tied product)*" (point 48). Tied selling can be both contractual and technical in nature.

[345] According to the above-mentioned Guidelines, the notion of "bundling" usually refers to the ways in which products are offered and priced by the dominant company.

[346] Decision 14-D-09 of 4 September 2014 on practices implemented by Nestlé, Nestec, Nestlé Nespresso, Nespresso France and Nestlé Entreprises in the espresso coffee machine sector.

[347] OECD, Data Portability, Interoperability and Digital Platform Competition, Reference note from the Secretariat, a December 2021 (link).

[348] Draft Commission guidelines on the application of Article 82 of the EC Treaty, 19 December 2005, paragraph 241.

[349] Commission decision of 24 March 2004, Case COMP/C-3/37.792 Microsoft; Case T-201/04, Microsoft Corp. Against Commission of the European Communities

workgroup servers under reasonable and non-discriminatory conditions. The reasoning was as follows:

- interoperability information was "*essential*"[350] for developing compatible products. In this case, some interoperability with the Windows domain architecture was possible, but it was too limited to allow Microsoft's competitors to remain viable in the market. The Court confirmed that it was sufficient to communicate technical documentation (the specifications of the corresponding protocols) and not give access to the Windows source code;
- there was a risk of eliminating all effective competition on the relevant market[351];
- the refusal had a negative effect on technical development to the detriment of consumers[352];
- Microsoft's refusal was not objectively justified. In this respect, the respondent company's arguments, based in particular on the intellectual property rights it held over the technology in question, were rejected[353].

571. In addition to the refusal to provide interoperability information, the competition authorities also examined the sharing of degraded or discriminatory information. For example, the *Autorité* raised competition concerns regarding 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)[354]. More recently, in May 2023, the *Autorité* found that Meta had failed to define transparent, objective, non-discriminatory and proportionate access criteria for its advertising verification partnerships. The *Autorité* has therefore ordered Meta to introduce new criteria for accessing and maintaining these partnerships[355].

572. Competition authorities can also penalise an operator in a dominant position for "*directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions*" (Article 102 (a) TFEU). The *Autorité* therefore penalised Google for the establishment and implementation of opaque and difficult-to-understand "Google Ads" rules, applied in an unfair and random manner[356]. The Paris Court of Appeal (*Cour d'appel de Paris*), which has confirmed the *Autorite's* decision in this case, recalled that to describe the practice as an abuse of a dominant position involves assessing whether the dominant undertaking's conduct was carried out to a "*reasonable extent"* [...], *and on the basis of an "objective justification"* [...] *by verifying that the conduct was both necessary and proportionate to achieve the objective of the dominant undertaking*"[357]. Furthermore, *"to demonstrate the existence of unfair trading conditions, the Autorité did not have to establish in the present case that the*

[350] Case T-201/04, cited above, paragraph 436.

[351] Case T-201/04, cited above, paragraph 620.

[352] Case T-201/04, cited above, paragraph 620.

[353] Case T-201/04, cited above, paragraph 711.

[354] Decision 22-D-12 of 16 June 2022 regarding practices implemented in the online advertising sector.

[355] Decision 23-MC-01 of 4 May 2023 on the request by the company Adloox for interim measures

[356] Decision 19-D-26 of 19 December 2019 regarding practices implemented in the online search advertising sector, upheld by the judgment of the Cour d’appel de Paris (Paris Court of Appeal) of 7 April 2022.

[357] Ruling of the Paris Court of Appeal (Cour d'appel de Paris) of 7 April 2022, 20/03811, point 130.

company derived an advantage from the practices"[358]. Lastly, the *Autorité* and the Court of Appeal took into account the *"extraordinary aspects*"[359] of Google's dominant position in the relevant market, which enabled it to establish rules considered as "*the "de facto standard" for advertisers wanting to purchase online search advertising services in France*"[360].

2. FAST, EFFICIENT TOOLS

573. In the course of the investigation, several players expressed concern about the length of the litigation procedures, which would make it impossible to solve their problems quickly enough.

574. Under the law governing anticompetitive practices, whether cartels or abuses, the *Autorité* has a number of procedural tools at its disposal to speed up its intervention in the market. On the one hand, pursuant to Article L. 464-1 of the French Commercial Code (*Code de commerce*), it can take interim measures to prevent imminent damage, in the event of serious and immediate harm to the interests of an economic sector, a company or consumers, or to the functioning of competition on the market. This procedure can be implemented quickly. For example, in April 2020, the *Autorité* decided to implement interim measures within five months in the Google related rights case[361], and in May 2023 vis-à-vis Meta in the online advertising verification sector[362] within seven months. In this way, the *Autorité* can prevent a potentially anticompetitive practice from seriously and irreparably harming competition or the company that is the victim of it.

575. On the other hand, when referred to, the *Autorité* may identify competition concerns and make the commitments proposed by the company in question to address these concerns binding (Article L.464-2 of the French Commercial Code (*Code de commerce*)). This procedure is particularly effective and generally leads to a faster resolution of the case. The *Autorité* can also assess the need to revise commitments (or sanction non-compliance), making it a particularly useful tool in the event of changes in the relevant market. In the Google AdTech case[363], Google also proposed commitments to improve the interoperability of Google Ad Manager services with third-party ad server platforms and supply-side platforms, and to phase out rules that favoured Google. More recently, Meta proposed commitments to provide non-discriminatory access to its online advertising programme for all its partners and provide access to a new application programming interface for advertising service providers[364].

576. These tools could therefore be usefully mobilised in the event of dominant players limiting migration and interoperability in the cloud sector.

[358] Ruling of the Paris Court of Appeal (Cour d'appel de Paris) of 7 April 2022, cited above, point 132.

[359] Decision 19-D-26, cited above, point 321, and ruling of the Paris Court of Appeal (Cour d'appel de Paris), cited above, point 103.

[360] Decision 19-D-26 cited above, point 321.

[361] Decision 20-MC-01 of 9 April 2020 regarding requests for interim measures by the Syndicat des éditeurs de la presse magazine, the Alliance de la presse d'information générale and others and Agence France-Presse.

[362] Decision 23-MC-01 of 4 May 2023 regarding the request by the company Adloox for interim measures

[363] Decision 21-D-11 of 7 June 2021 regarding practices implemented in the online advertising sector.

[364] Decision 22-D-12 of 16 June 2022 regarding practices implemented in the online advertising sector.

B. COMPETITION LAW AND CARTELS

1. ANTITRUST ISSUES CONCERNING AGREEMENTS AND PARTNERSHIPS BETWEEN CLOUD PLAYERS

577. Stronger partnerships between cloud service providers or between cloud service providers and integrators, or specific interoperability agreements between certain cloud and SaaS players, could raise issues with regard to antitrust law on the basis of Articles 101 TFEU and L. 420-1 of the French Commercial Code (*Code de commerce*), whether they are horizontal or vertical agreements.

- Over the past few years, a wide variety of groupings and associations, with or without the creation of a common legal structure, have been formed or are in the process of being formed between cloud service providers exclusively or also integrating other companies, in particular other digital players or manufacturers. These include:
- joint structures between cloud operators to present "trusted cloud" offerings (see Part 1);
- technological partnerships between major data-related software vendors and cloud service providers; for example, AWS and Salesforce (a specialist in customer management solutions) are strategic partners on a global scale, with the aim of securely connecting data and workflows[365]. This is also the case for SAP, one of the market leaders in business software, and Google Cloud[366]. 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[367];
- alliances or technological partnerships between integrators and the majority of cloud service providers, notably hyperscalers (see Part I.C); depending on the context and objectives of the partnership, these alliances may involve mutual collaboration agreements to jointly propose service offerings and cloud solutions to common customers, the purchase and resale of their cloud solutions, the integration of their cloud solutions into the integrator's services, or the use of providers' expertise around their cloud solutions as subcontractors;
- specific partnerships in certain sectors. This is the case, for example, in the automotive sector, as illustrated by the Renault-Nissan Group's partnership with Microsoft to make Azure the automotive group's platform, or the partnership between Stellantis and AWS[368] (see Part II. D 3).

[365] ttps://aws.amazon.com/featured-partners/salesforce/ (accessed on 16 February 2023).

[366] https://news.sap.com/france/2018/10/sap-et-google-cloud-une-complementarite-technologique-agile-et-innovante-au-service-des-entreprises/.

[367] Microsoft Azure and Oracle press release, Microsoft and Oracle announce interconnection of Microsoft Azure and Oracle Cloud systems, 5 June 2019, link.

[368] Some partnerships may nevertheless raise competition concerns, as shown by the Bundeskartellamt's recent statement of objections concerning Google's licensing practices for in-vehicle infotainment systems (linked in particular to Google Maps) (link).

578. The investigation revealed that these alliances may raise concerns, particularly from the point of view of commercial or technical customer lock-in. The fact, on the one hand, that these entities group together autonomous and sometimes competing companies and, on the other hand, that their operation implies contact between these same companies exposes them, and their members, to risks with regard to the rules prohibiting cartels. It is important to recall in this respect that while a certain degree of concertation between companies through these entities is possible, this concertation must not have an anticompetitive purpose or effect. In particular, concertation between cloud service providers through these entities regarding the prices charged could be considered as having an anticompetitive purpose.

2. STANDARDISATION AGREEMENTS BETWEEN CLOUD SERVICE PROVIDERS

579. Standardisation solutions, which at first glance encourage interoperability and hence switching provider, could, in some cases, become problematic. If this practice is carried out by several entities acting in concert, prevents the emergence of alternative solutions and paralyses innovation through technical lock-in practices, it could entail risks with regard to the rules prohibiting illegal cartels. This will be all the more the case if the situation leads to an increase in the price of the favoured solution.

580. The *Autorité* has already noted in this sense, in its aforementioned 2015 opinion[369], that standardisation can restrict competition "*if it enables the approval of a standard biased in favour of certain market players, who can then use it to erect a barrier to entry for competitors or innovators*". For example, certain standards could be imposed because they are used by the market leaders, who may have the ability to control the evolution of these solutions, with the other players needing to assume the costs of compliance with these standards. This concern is shared by a number of industry players. According to one cloud service provider: "*A player with significant market power could therefore be tempted to promote a solution initially presented as open in order to establish it de facto as a market standard and thus capture a significant number of customers, before progressively locking access to this technology to make users captive to its own services. This strategy of tactical openness, which consists of opportunistically promoting an apparently open solution before gradually reintroducing frictions leading to a market lock-in effect, is particularly dangerous for the long-term functioning of the sector. It is likely to have an impact on the competitive functioning of the market, as well as on innovation, particularly if these standards are deployed on both the B2B and B2C clouds (for example, a standard linked to Internet pages or services)*".

C. MERGER OPERATIONS

581. The scenarios described above could be reinforced by an aggressive acquisition policy by companies already present in the cloud sector, in order to strengthen their position in an identified cloud market or a related market. The *Autorité* has therefore focused on takeover strategies and mergers that may contribute to reinforcing and accelerating mergers in the cloud sector. Lastly, the creation of new entities in the form of joint ventures bringing

[369] Opinion 15-A-16 of 16 November 2015 reviewing standardisation and certification processes in the light of competition law.

together major players in the sector to offer products specially designed to cover new market segments is a form of merger that is particularly likely to raise competition concerns.

1. Acquisition transactions

582. In recent years, there have been a number of major transactions involving cloud service providers around the world, some of which have been subject to scrutiny by competition authorities, such as IBM's $34 billion acquisition of software provider Red Hat, an expert in open-source solutions, in July 2019[370].

583. Generally speaking, the supervisory authorities' merger analysis must ensure that the transaction does not harm competition. While a merger can have positive effects, particularly in terms of efficiency gains, it can also give rise to major competition problems. The assessment of a merger generally depends on the type of merger involved, whether it is horizontal (between competitors in the same market), vertical (between entities operating in markets at different levels of the value chain) or conglomerate (between entities operating in different but related markets).

584. Among the positive effects, acquisitions can enable a provider to improve its offering, close the gap with established competitors or expand into new segments. Examples include IBM's aforementioned acquisition of Red Hat and Turbonomic, a company specialising in artificial intelligence-based application management and network performance, in 2021, to strengthen its hybrid cloud offering. In 2020, Microsoft acquired Affirmed Networks (a specialist in 5G network virtualisation) and Metaswitch (a manufacturer of virtualised network software), to offer services to the telecoms sector *via* the *Azure for Operators* offering.

585. However, certain acquisitions can have a negative impact on competition. For example, a merger can have unilateral effects when it involves competitors who are sufficiently close to each other to eliminate a major source of competitive pressure. Increased barriers to expansion can also result, for example, from the acquisition of a company whose purpose was to facilitate interoperability. Similarly, such transactions can also lead to the reinforcement of conglomerate effects (see Part II).

586. During the public consultation, a number of operators expressed concerns about possible mergers in the cloud industry. Among the main risks identified, they mentioned the reduction in the number of companies, potential bundled or tied selling, the drying up of innovation and alternatives for clients, and potential price increases. An operation can also enable a player to acquire key market assets, such as a specific technology or particularly expert human resources, which can also act as a brake on competitors' expansion.

587. In addition, a number of respondents believed that the major cloud players have privileged information at their disposal, in addition to their substantial investment capacities. According to some, the takeover strategies of certain hyperscalers could thus be guided by privileged access to data on their cloud, particularly that acquired *via* their marketplace (see Part IV.B). This knowledge can lead the provider to rapidly acquire these solutions and integrate them into its own services. This type of strategy can have a number of negative effects, such as removing from the market players who could have competed with the hyperscaler in part of its market. This could also contribute to the creation of proprietary ecosystems and the locking-in of the customers who used these technological tools. Several companies

[370] Commission decision of 27 June 2019, case COMP/M.9205, *IBM/Red-Hat*.

mentioned cases where technology solutions that could previously be integrated with multiple providers were transformed into proprietary technologies after a take-over.

588. One provider also pointed out that the main hyperscalers may have a strategy of acquiring stakes or even acquiring their main customers, in order to secure their markets and economies of scale. Transactions of a conglomerate nature in other sectors would therefore be likely to affect competition in the cloud market by modifying customers' incentives to use other providers.

589. The consultation revealed that a dynamic of mergers seems to be underway in the cloud sector, and could continue over the next few years. In the French market, a number of recent takeovers are seen as a sign of this dynamic, such as the 2021 acquisition of cloud services provider Ikoula by enterprise telecoms and cloud operator Sewan, or the acquisition of Linkbynet, which specialises in outsourcing[371], managed IT services and the cloud, by Accenture in the same year.

590. A number of players also expressed concern about the large-scale buyout plans already announced. An ongoing case is the proposed $61 billion takeover of VMware[372] by the US group Broadcom, which is currently being examined by several competition authorities, including the European Commission[373]. In particular, Cigref members believed that Broadcom's takeover of VMware, considered dominant in the virtualisation market, could lead to a deterioration in the quality of VMware's virtualisation products and services, and to higher prices. In their view, Broadcom is an "*aggressive player, multiplying practices that could be qualified as abusive and unfair*"[374], which could therefore modify VMware's practices after the buyout, as customers have already seen following previous Broadcom takeovers, notably CA Technologies and Symantec.

591. Furthermore, Microsoft's takeover of Activision Blizzard, which has raised concerns about the emerging cloud gaming market, has prompted contrasting responses from competition authorities. According to the CMA's analysis[375], Microsoft already accounts for around 60-70% of global cloud gaming services and has other significant strengths in the cloud gaming arena through its ownership of Xbox, the leading PC operating system (Windows), and a global cloud infrastructure (Azure and Xbox Cloud Gaming). According to the CMA, in the absence of a merger, Activision would have begun delivering games via cloud platforms i*n* the foreseeable future. The CMA therefore prohibited the proposed acquisition, fearing that the deal would alter the future of the fast-growing cloud gaming market, leading to reduced

[371] According to Decision 15-DCC-02 of 22 January 2015 regarding the acquisition of sole control of the user and workstation support business of Atos A2B and Atos Infogérance by Proservia WorkStation Services: *"Global management services, also known as 'outsourcing' or 'systems management services', include operational services, applied management, help desk management, business continuation, asset management, outsourcing and evolutionary leasing*" (paragraph 8).

[372] American software solutions company specialising in virtualisation.

[373] Proposed merger notified to the European Commission on 15 November 2022 (Case M.10806 - Broadcom/VMware). The European Commission informed Broadcom of its preliminary conclusion that its proposed acquisition of VMware could restrict competition in the market for certain hardware components interoperable with VMware's virtualisation software on 12 April 2023.

[374] Cigref press release, "Broadcom’s takeover of VMware: customers are alarmed about a drift in practices; Cigref and its partners alert the merger control authorities", 27 June 2022 (link).

[375] CMA final report on the acquisition project, 26 April 2023 (link).

innovation and less choice for UK gamers in the years to come. The Commission[376], for its part, cleared the proposed acquisition, subject to Microsoft's compliance with ten-year licensing commitments enabling European consumers to access Activision Blizzard's current and future games free of charge from the cloud game streaming service of their choice. The Commission considered that Microsoft would not be in a position to harm competing consoles and multi-game subscription services.

2. ACQUISITION STRATEGIES FOR CLOUD SERVICES COMPANIES

592. The *Autorité* has observed a significant difference in acquisition strategies between cloud service providers. While the largest cloud service providers, particularly the American ones, have all made acquisitions in recent years, this has rarely been the case on the part of European operators. While Microsoft acquired 25 companies between 2018 and 2021 to enhance its Azure, Microsoft 365 and Dynamics 365 offerings, Scaleway and 3DS Outscale did not acquire any companies during this period.

593. It should be noted that the majority of transactions in this sector have not been subject to merger control proceedings. This is due in particular to the fact that the turnovers of the acquired companies were generally below the notification thresholds set at national[377] and European[378] level. However, this lack of control does not mean that certain acquisitions do not have damaging effects on competition, leading, for example, to increased lock-in with certain providers and, consequently, mergers in the sector.

594. As a reminder, the Merger Regulation gives the Commission exclusive competence to examine mergers with a European dimension, as defined by the application of combined thresholds based on turnover. Nevertheless, several referral mechanisms provided for in EU Regulation 139/2004 enable Member States and companies whose transactions do not exceed European and/or national thresholds to request that the operation be examined by the European Commission. Mergers that do not have a Community dimension, but should be notified in at least three Member States, may be referred to the Commission at the request of the companies pursuant to Article 4(5) of Regulation 139/2004.

595. With regard to transactions that fall below both Community and national thresholds, the renewal of the doctrine applied by the European Commission to referrals under Article 22 of Regulation 139/2004 provides an appropriate response for examining operations that elude the control of national competition authorities despite the harmful effects they may have on competition. The Commission recently announced that, under certain circumstances defined in its guidelines[379], it would accept referrals by national authorities, under Article

[376] Commission press release, Mergers: Commission clears acquisition of Activision Blizzard by Microsoft, subject to conditions, 15 May 2023 (link).

[377] The French Commercial Code (Code de commerce) (Article 430-2) provides for the notification of a transaction if the total global turnover of all the parties involved exceeds €150 million and the total turnover in France of at least two of the companies involved exceeds €50 million.

[378] Article 1 of Regulation 139/2004 on the control of concentrations between undertakings stipulates that a merger has a Community dimension when certain turnover thresholds are met.

[379] Commission guidelines on the application of the referral mechanism set out in Article 22 of the Merger Regulation to certain categories of cases (2021/C 113/01). These guidelines set out the main principles applicable to the referral of cases not subject to the notification obligation under the legislation of the requesting Member State(s). Pursuant to Article 22 of the above-mentioned Regulation, the Commission will assess in

22, of transactions that do not have a European dimension and that fall below the notification thresholds at national level[380]. In September 2022, this mechanism led the Commission to prohibit Illumina's acquisition of Grail, a biotech company specialising in the early detection of cancer[381]. It should make it easier for competition authorities to detect and intervene in mergers by cloud sector companies that fall below national notification thresholds.

596. The Article 22 mechanism could be strengthened, particularly in the cloud sector, by the Digital Markets Act. Article 14 of this Act introduced the obligation for gatekeepers to inform the Commission of any proposed merger where the acquired company provides essential platform services or any other service in the digital sector or that enables data to be collected. As already seen (see Part I.E), since the main cloud service providers are likely to be designated as gatekeepers, and their cloud services as essential platform services, the Commission could be aware of sensitive acquisition projects for the cloud sector and exercise greater vigilance. In addition, the Commission will be able to share this information with the competent authorities of the Member States concerned by the merger, thus opening up the possibility for the national competition authority to refer the transaction to the Commission.

597. In addition to these measures, the CJEU recently confirmed the possibility of examining mergers below the European and national thresholds with regard to the possible reinforcement of a dominant position, in line with the Continental Can case law and doctrine to date[382]. According to a recent ruling by the CJEU, Article 102 TFEU can be applied to a merger operation below the European and national control thresholds, provided that certain conditions are met: "*In particular, it is for the authority in question to verify that a purchaser who is in a dominant position on a given market and who has acquired control of another undertaking on that market has, by that conduct, substantially impeded competition on that market. In that regard, the mere finding that an undertaking's position has been strengthened is not sufficient for a finding of abuse, since it must be established that the degree of dominance thus reached would substantially impede competition, that is to say, that only undertakings whose behaviour depends on the dominant undertaking would remain in the market (see, to this effect, judgments of 21 February 1973, Europemballage and Continental Can v Commission, 6/72, EU:C:1973:22, paragraph 26, and of 16 March 2000, Compagnie maritime belge transports e. a./Commission, C-395/96 P and C-396/96 P, EU:C:2000:132, paragraph 113).*" [383]

particular whether the transaction is likely to affect trade flows between Member States, taking into account, for example, the location of (potential) customers or the collection of data in several Member States (paragraph 14). Furthermore, the aspects to be taken into account in deciding whether the transaction threatens to significantly affect competition may include the creation or strengthening of a dominant position on the part of one of the companies concerned (paragraph 15). Other factors may be taken into consideration, such as cases in which the company is a major innovator or exerts significant competitive pressure (paragraph 19).

[380] On this subject, see the Autorité's press release, "*The Autorité welcomes the announcement by the European Commission, which will henceforth allow national competition authorities to refer sensitive merger transactions to it for examination, including when they are not subject to national merger control*", published on 15 September 2020 (link).

[381] This decision is pending appeal before the CJEU.

[382] CJEU, 21 February 1973. - Europemballage Corporation and Continental Can Company Inc. v Commission of the European Communities.

[383] CJEU ruling, 16 March 2023, C-449/21, Towercast SASU v/Autorité de la concurrence, paragraph 52.

598. The analysis of these cases must take into account their anticompetitive effects, and in particular the difficulty, in some cases, of repairing *ex post* the negative effects caused by a merger. Ongoing discussions at European level[384] concerning the analysis of mergers in the digital sector - aimed in particular at ensuring that characteristics such as strong network effects, advantages linked to data access, the risks of a shift towards a monopoly situation ("tipping") or the creation of ecosystems are taken into account - may provide further input for developing the analysis of European competition authorities in the cloud sector.

599. In addition, the acquisition of minority shareholdings in the capital of a company which, if theyare subject of agreements, could justify the application of Article 101 TFEU[385], and the acquisition of assets, such as exclusive patent licences, which could be examined from the angle of Article 102 TFEU[386], could also be a subject of interest.

3. THE CREATION OF JOINT VENTURES

600. Lastly, the creation of new entities in the form of joint ventures bringing together major players in the sector to offer products specially designed to cover new market segments, like "trusted cloud" offerings, is a form of merger particularly likely to raise competition concerns.

601. These new entities could in fact group together companies that already enjoy significant competitive advantages and consequently limit the ability of other, less powerful players to compete with them. Depending on competitive constraints and the ability of other players to develop competitive offers, these entities could also have significant market shares and be in a position to exercise market power.

602. During the investigation, a number of industry players expressed concerns regarding these projects[387]. In particular, they pointed to the risks to competition raised by the communication and marketing resources used even before the creation of the joint ventures, the commercial launch of the offerings and the emphasis placed on obtaining the "trusted cloud" label (requiring their SecNumCloud certification). In their view, this announcement effect could give a major advantage to "trusted cloud" offerings, with many customers able to pre-select these offerings to the detriment of those of other players also under development. In this context, some providers have decided not to develop "trusted cloud" offerings for the time being.

[384] In particular, the European Commission organised a workshop on digital mergers on 13 December 2022 (link).

[385] Judgment of the Court (Sixth Chamber) of 17 November 1987. - British-American Tobacco Company Ltd and R. J. Reynolds Industries Inc. against Commission of the European Communities - Competition - Rights of complainants - Participation in the capital of a competing company. - Joined cases 142 and 156/84.

[386] Ruling of the Court of First Instance of 10 July 1990. - Tetra Pak Rausing SA against Commission of the European Communities - Competition - Relationship between Articles 85 and 86 - Benefit of a block exemption and applicability of Article 86. - Case T-51/89.

[387] Press release of 6 October 2021, Thalès and Google Cloud announce a strategic partnership to jointly develop a "trusted cloud" offering in France (link); Capgemini and Orange press releases of 22 June 2022, Capgemini and Orange announce that Bleu will start engaging with future customers by the end of 2022, (link and link).

603. Other players, both customers and providers, have nonetheless emphasised the value of these initiatives for the competitive process, considering them to be akin to the creation of new offers, with a qualitative gain responding to the demand for better data protection emanating from certain players.

604. The Commission has just cleared the creation of Bleu, the joint venture between Capgemini and Orange based on Microsoft Azure technologies, as mentioned above. It concluded that the proposed transaction would not give rise to any competition concerns under the Merger Regulation, as there would be no overlap between the companies' activities as a result of the transaction. The Commission also found that vertical relationships between upstream and downstream markets, as well as conglomerate relationships between companies, would not raise competition concerns[388] (see Part I).

D. ABUSE OF ECONOMIC DEPENDENCE

605. Under Article L. 420-2, par. 2 of the French Commercial Code (*Code de commerce*), the abusive exploitation by a company or group of companies of the state of economic dependence in which a customer or provider finds itself is prohibited, when this is likely to affect the functioning or structure of competition. More specifically, "*these abuses may include refusals to sell, tied selling, discriminatory practices under Articles L. 442-1 to L. 442-3 or range agreements.*"

606. While the concept of abuse of economic dependence ("abus de dominance économique") has no equivalent in EU law, this infringement is compatible with it, as EC Regulation of the Council 1/2003 of 16 December 2002 on the implementation of the competition rules laid down in Articles 81 and 82 of the Treaty (now Articles 101 and 102 TFEU) states that, "*Member States shall not be precluded from adopting and applying on their territory stricter national laws which prohibit or sanction unilateral conduct engaged in by undertakings*".

607. This infringement, which was recently introduced in several countries, such as Belgium in 2020[389], differs from abuse of a dominant position in several respects.

608. Firstly, while in the context of the application of Article 102 TFEU and Article L. 420-2, paragraph 1, of the French Commercial Code (*Code de commerce*), the determination of the relevant market is, in principle, a prerequisite for the assessment of the possible existence of a dominant position on the part of the company concerned, this is not the case with regard to abuses of economic dependence. The purpose of defining the relevant market in the case of prohibition of abuse of a dominant position is to define the perimeter within which the undertaking is able to behave to an appreciable extent independently of its competitors, customers and consumers. However, economic dependence is not assessed on the basis of a company's position in a given market, but on the basis of the specific nature of its trade relations with upstream or downstream partners.

609. Secondly, abuse of economic dependence requires three cumulative conditions to be met: the existence of an economic dependence by one company on another, the abusive

[388] Commission press release of 13 June 2023, Mergers: Commission approves creation of joint venture by Capgemini and Orange in the field of sovereign cloud (link).

[389] https://economie.fgov.be/fr/themes/entreprises/protection-des-entreprises/abus-de-dependance-economique.

exploitation of this situation, and an actual or potential effect on the functioning or structure of competition. While demonstrating the last two conditions does not, as a general rule, raise any particular difficulties, the situation of economic dependence must be strictly assessed. In a ruling dated 12 October 1993, Competition, 91-16988 and 91-17090, the French Supreme Court (*Cour de cassation*) defined four cumulative criteria for determining an economic dependence as follows: "*if the existence of an economic dependence is assessed by taking into account the reputation of the provider's brand, account should also be taken of the size of its share of the market in question and of the reseller's turnover, as well as the impossibility for the latter to obtain equivalent products from other providers*".

610. Although rarely used in the decision-making practice of the *Conseil de la concurrence* and then the *Autorité,* this infringement was recently established by the *Autorité* to punish Apple[390]. In this case, Apple's alleged abuse of economic dependence, with regard to its specialised high-end distributors (known as APR for Apple Premium Reseller), involved supply difficulties which put them at a disadvantage compared to Apple's own shops. The APRs' economic dependence resulted from their inability to find a comparable technical and economic alternative to their relationship with Apple. For the *Autorité*, followed by the Court of Appeal (*Cour d'appel*)[391], no dominant position was demonstrated in an abuse of economic dependence: "*economic dependence is not assessed on the basis of a company's position in a given market, but on the basis of the specific nature of its trade relations with upstream or downstream partners* (paragraph 554).

611. Abuse of economic dependence can be used to apprehend abusive contractual practices by digital operators, especially the largest cloud service providers. The relationship of dependence between hyperscalers and their customers is described in detail above (see Part IV.A.). In its June 2020 study on e-commerce, the *Autorité* also noted the appropriateness of this qualification for marketplace practices[392].

E. THE LAW ON RESTRICTIVE COMPETITIVE PRACTICES

612. As the cloud raises a wide range of legal risks, some authors[393] have questioned whether these issues should be considered in a broader sense than the sanctioning of abuses of a dominant position or abuses of economic dependence, for example from the angle of restrictive competition practices. Its implementation falls primarily under the jurisdiction of the Directorate General for Competition Policy, Consumer Affairs and Fraud Control

[390] Decision 20-D-04 of 16 March 2020 regarding practices implemented in the sector of distribution of Apple branded products: This Decision was confirmed on this point by the Paris Court of Appeal (Cour d'appel de Paris) in a ruling dated 6 October 2022.

[391] According to the Paris Court of Appeal (Cour d'appel de Paris), "*With regard to Apple's market share, it should be recalled, as the contested decision rightly did, that the existence of a dominant position is not required for the application of Article L.420-2, paragraph 2, of the French Commercial Code (Code de commerce). The fact that, in its previous practice, the Autorité has only sanctioned operators in a dominant position on this basis does not rule out its application to a company with relative power over its partners as a result of strong bargaining power based, in particular, on its reputation*" (paragraph 545).

[392] Autorité de la concurrence, Report on Competition and e-commerce, page 119.

[393] In a working paper devoted to the cloud, Fréderic Marty wrote: *"The essential point, which is clearly apparent in the case of the cloud, is linked to the specific issue of abuse of relative dominance and the question of fair trade relations. In other words, it is important to consider both big and little competition law."* (link).

(*Direction générale de la Concurrence, de la Consommation et de la Répression des frauds*, DGCCRF). As such, the DGCCRF can sue companies that infringe the legislation on trade practices to be sanctioned. In particular, the Directorate may ask the court to order the cessation of the practices, the annulment of the clauses or contracts, which are the instruments of the abusive practice, the recovery of the sums unduly received, the reparation of any damage as well as the imposition of a civil fine. However, action may also be taken by the President of the *Autorité* if, in the course of business within their jurisdiction, they find that a restrictive practice has been infringed.

613. By way of illustration, contractual clauses imposed by cloud service providers on their co-contractors, which subject the latter to "*obligations creating a significant imbalance in the rights and obligations of the parties*", or enable them to obtain an "*advantage corresponding to no consideration or manifestly disproportionate to the value of the consideration granted*", as well as any unilateral practices with the same characteristics, could be qualified as restricting competition under Article L. 442-1 of the French Commercial Code (*Code de commerce*)[394]. The same would apply if the cloud service provider were to abruptly terminate established trade relations without sufficient notice.

614. These provisions, which are based on the principle of fair trade relations, do not require the prior definition of a relevant market or the establishment of the perpetrator's dominant position. Sanctioned *per se*, they do not require the demonstration of any effect on the market. Sanctions for restrictive trade practices are currently imposed by commercial courts and specialised judicial courts. Cases may be referred to these courts by any interested party, as well as by the Public Prosecutor, the Minister for the Economy or the Chairperson of the *Autorité*.

615. Under Article L. 442-4 of the French Commercial Code (*Code de commerce*), the courts may be asked to issue injunctions to cease the practices in question, compensate for damages, cancel the clauses in question, reimburse undue payments and impose civil fines. The judge responsible for dealing with urgent matters can also order the cessation of practices as a matter of urgency.

616. These provisions, initially used in the mass retail distribution sector, have been successfully invoked for several years now by the French Minister of Economy against major companies

[394] In its version in force on 1 April 2023, this article stipulates: "*The perpetrator shall be liable and obliged to compensate for any damage caused by, in the context of commercial negotiation, the conclusion or performance of a contract, any person engaged in production, distribution or service activities:*

1° obtaining or attempting to obtain from the other party an advantage for which there is no compensation or which is clearly disproportionate to the value of the compensation given;

2° submitting or attempting to submit the other party to obligations, creating a significant imbalance in the rights and obligations of the parties; (...)

II - Any person engaged in the production, distribution or provision of services who suddenly breaks off, even partially, established trade relations, without prior written notice which takes into account, in particular, the duration of the trade relations, with reference to trade practices or interprofessional agreements, and, for the determination of the price applicable for its duration, the economic conditions of the market in which the parties operate (...) shall incur liability and be obliged to compensate the damage caused (...)".

active in the digital sector, such as Booking[395], Expedia[396], Google[397], Apple[398] and Amazon (see below).

617. In 2019, Amazon was sentenced by the Paris Commercial Court (*Tribunal de commerce de Paris*)[399] for imposing several unbalanced clauses on its commercial partners in the general terms and conditions of use of its marketplace. According to the court, the submissiveness of third-party vendors was demonstrated by a body of evidence, such as the existence of standard contracts, a highly unbalanced economic power relationship between the parties marked by dependency, and the essential role of the co-contractor. For example, the sanctioned clauses included those allowing Amazon, at its sole discretion, to amend its contracts without prior notice, terminate or suspend the contract without prior notice, and exempt itself from liability for certain foreign shipments.

618. It should be noted that, since December 2020, under III of Article L. 470-1 of the French Commercial Code (*Code de Commerce*), the French Minister of Economy has been able to issue an administrative injunction against companies to cease restrictive practices subject to a periodic penalty payment. While it takes a long time to refer a case to the courts, the aim is for companies to comply as quickly as possible. This action, again successfully taken against Amazon[400], will undoubtedly be used very frequently in the future by the DGCCRF in the digital sector, and could also be used in the cloud sector.

Competition Law responses

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 in the cloud sector. Examples include the Google Shopping case in 2021 (in which the General Court of the European Union clarified the issue of discrimination and 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.

The *Autorité* also has effective and rapid procedural tools at its disposal, such as interim measures and commitments.

From the point of view of the competition law and cartel, a wide range of groups and associations of cloud service providers have been formed in recent years or are being formed, with or without the creation of a common legal structure, including:

– joint structures between cloud operators to present "trusted cloud" offerings;

[395] Paris Commercial Court (Tribunal de commerce de Paris), First chamber, General Cause List 2014027403, 29 November 2016 (link).

[396] Paris Court of Appeal (Cour d'appel de Paris), French Minister of Economy against Expedia, General Cause List 15/18784, 21 June 2017 (link).

[397] https://www.economie.gouv.fr/files/files/directions_services/dgccrf/presse/communique/2018/cp-google-apple.pdf.

[398] https://www.economie.gouv.fr/files/files/directions_services/dgccrf/presse/communique/2018/cp-google-apple.pdf.

[399] Paris Commercial Court (Tribunal de commerce de Paris), General cause list 2017050625, 2 September 2019 (link).

[400] Press release, the Directorate General for Consumer Affairs, Competition and Fraud Prevention asks Amazon to make a periodic penalty payment of 3.3 million euros for a delay in complying with contractual conditions on Amazon.fr, 7 December 2022 (link).

- technological partnerships between major data-related software providers and cloud service providers. In 2019 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 service providers, especially hyperscalers.

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. Such agreements could be analysed to assess whether, for example, they are likely to promote innovation or economic efficiency and check that they are not likely to reduce competition.

Standardisation solutions, which at first glance promote interoperability and therefore provider switching could also, in some cases, become problematic. If this practice is carried out by several entities acting in concert, prevents the emergence of alternative solutions and paralyses innovation through technical lock-in practices, it could entail risks with regard to the rules prohibiting cartels, particularly if it leads to an increase in the price of the favoured solution.

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 service 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 being checked by several competition authorities and Microsoft's take-over of Activision Blizzard, which has raised concerns about the emerging cloud gaming market and led to contrasting responses from the competition authorities.

During the public consultation, a number of operators expressed concerns about possible mergers in the cloud industry. Among the main risks identified, they mentioned the reduction in the number of companies, potential bundled or tied selling, the drying up of innovation and alternatives for clients, and potential price increases. Several companies also mentioned cases where technology solutions that could previously be integrated with multiple providers 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 service providers, particularly the American ones, have all made acquisitions in recent years, this has rarely been the case 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 raised by the communication and the marketing resources deployed to launch their offers and obtain the "trusted cloud" label.

Finally, since the cloud raises a wide range of legal risks (impact on customers and competitors, structural failings in the sector, potentially abusive contractual conditions), it may be appropriate to consider these issues from a broader angle than the sanction for abuses of a dominant position.

These infringements could also be sanctioned by the *Autorité* on the grounds of abuse of economic dependence. The *Autorité* used this legal basis to sanction Apple in 2020.

The application by the Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF) of provisions relating to restrictive competition practices could actually be justified, notably from the perspective of significant imbalance or unrequited advantage.

VI. Other responses in the event of market failures

1. TECHNICAL MARKET FAILURES

619. The *Autorité* notes that the competitive functioning of the cloud market does not currently allow the optimal allocation of resources. While technical solutions exist to facilitate switching provider or use of the multi-cloud (standard services or open-source solutions, for example), incumbent providers, particularly hyperscalers, are not necessarily encouraged to develop the most technologically high-performance solutions or charge the best price. Furthermore, joint initiatives to develop common standards are encountering implementation difficulties, which justifies the regulatory intervention envisaged at European level, notably in the proposed data regulation.

a) Challengers have more incentive to develop interoperable tools

620. Smaller cloud service providers, known as "challengers", have a particular incentive to develop interoperable solutions to meet customer demand and compete with more established providers.

621. The ability for a customer to switch to a different provider or use the multi-cloud opens up growth opportunities for providers competing with hyperscalers. Aware of the risk of lock-in within hyperscaler ecosystems, customers may be tempted to use providers offering maximum freedom from a technical point of view, in particular through the use of solutions that are as open as possible and facilitate reversibility and interoperability. These solutions include open-source technologies such as containers or open application programming interfaces, even if they have their limitations (see Part IV).

622. This strategy of opening up to compete with hyperscalers was confirmed by market players:

- one cloud service provider confirmed that: "*Interoperability and multi-cloud present real growth opportunities for the market in general, and for alternatives to hyperscalers in particular*";
- for another provider: "*multi-cloud architectures will enable companies to grow faster and use other providers*";
- lastly, one customer asserted that "*if they want to exist, players in a challenger position are forced to offer cloud services with a standard API that enables customers to move from an on-premise instantiation of their workload to an on-cloud instantiation without having to rewrite the source code*".

623. All alternative cloud service providers are therefore promoting a proactive strategy of openness for their customers. For example, one stated: "*we have chosen to use open-source solutions or well-established protocols for our products, with the aim of being as interoperable as possible*", while another confirmed "[t]*here are no technological lock-ins for our customers*", and yet another: "*our operation implies that the customer has a great deal of freedom to operate a similar service with other cloud service providers, thanks to our respect for open standards*".

624. Of course, hyperscalers are also communicating about the range of services and tools available to customers wanting to migrate out of their environment or adopt multi-cloud strategies. For example, a hyperscaler may facilitate interoperability by making services such

as Kubernetes available, use various standard protocols such as Linux operating systems, or allow third parties to use their public application programming interfaces. Another hyperscaler confirmed: "*technologies such as Kubernetes and other open-source services are widespread in public clouds (e.g. Linux, Chef, nodeJS, Drupal, MongoDB) and give customers* [...] *the assurance that if they build their solutions using such services, they will be able to migrate their workloads to other public clouds*."

625. However, hyperscalers do not have the same incentives as their competitors to develop tools that encourage their customers to migrate to competing providers. A provider in a position of strength is unlikely to voluntarily adopt a policy of interoperability, whose aim is to reduce barriers to entry and expansion and promote competition that erodes its market power. As one competing cloud service provider said: "*the initial finding we can share is that dominant players like AWS have no interest in giving up market share*". Several customers confirmed that the major cloud service providers are not necessarily looking to offer standardised solutions for accessing their cloud services. According to one: "*in terms of APIs, each major cloud player offers its own API and has nothing to gain from standardisation, which favours competition and customer volatility*". For one cloud service provider, highlighting interoperable services such as Kubernetes can be a loss leader that ultimately locks users in: "*if a customer who starts out using Kubernetes wants to scale up*[401] *and use their data, it is highly likely that they will subscribe to non-interoperable hyperscaler cloud services associated with technical barriers to migration*".

b) Self-regulation initiatives have failed to establish common technical standards

626. To resolve the barriers to migration and interoperability in the sector, national and European authorities[402] have so far favoured an approach based on the introduction of non-binding legal instruments. However, the adoption of common standards by market players is proving slow and difficult.

627. The introduction of standards is likely to encourage customer migration, particularly towards the most homogeneous services. They lower the barriers to entry and open up access to new markets by establishing clear and effective rules for all the parties concerned. By facilitating the compatibility and interoperability of the different products and services, the adoption of standards can have a pro-competitive effect by promoting diversity of provision and enabling customers to compare different products or services more easily, thus encouraging competition on the merits[403]. Standards can therefore help combat customer lock-in, as they make it easier to switch from one provider to another, or use several providers simultaneously. However, the application of standards could be counterproductive if they were to apply to differentiated products subject to innovation.

628. While there are no formally binding standards in the cloud sector, several *de facto* standards have emerged. This is the case, for example, with open-source (Kubernetes initially

[401] Describes the ability to dynamically increase or decrease resources (e.g. a website more frequently visited at Christmas).

[402] The Government announced five new measures on 12 September 2022, among them the strengthening of the SecNumCloud visa and "*the implementation of a harmonised European cyber security certification scheme for cloud services*" (link).

[403] Opinion 15-A-16 of 16 November 2015 reviewing standardisation and certification processes in the light of competition law, paragraph 3.

developed by Google Cloud) or proprietary (simple storage service (S3) initially developed by AWS), which have been adopted by all players.

629. In recent years, initiatives have also been developed to set standards in the sector[404]. At European level, the association Gaia-X, initially founded by 22 French and German organisations and supported by their respective governments, aims to guarantee data sovereignty, availability, interoperability and portability, and to promote transparency. A series of documents[405] was published on 21 April 2022 to define the latest version of technical and non-technical standards to be shared by market players in order to achieve Gaia-X's initial objective[406]. However, according to the majority of stakeholders, the implementation of the standards set out in these documents is not yet an operational reality. Furthermore, the participation of international conglomerates in technical working groups, and their supposed desire to slow down or complicate discussions, is widely criticised. This is the main reason why Scaleway announced in November 2021 that it had not renewed its membership of the project[407].

630. Another European initiative is "SWIPO" (Switching Cloud Service Providers and Porting Data), a multi-stakeholder group whose aim is to publish codes of conduct based on the principles of transparency, interoperability and open standards, in application of Article 6 ("Porting of data") of the Regulation on the free flow of non-personal data in the European Union[408]. The aim is to enable business users to make informed choices and easily compare service and porting of data offerings. Codes of conduct must "*also make it clear that reliance on providers is not an acceptable trade practice*"[409]. Lastly, Article 6 encourages service providers to complete the development of the codes of conduct by 29 November 2019 and to effectively implement them by 29 May 2020. SWIPO has published two codes of conduct on data portability, one covering SaaS[410] services (8 July 2020) and the other covering IaaS[411] services (27 May 2020). Once again, the majority of stakeholders criticise the slowness of the work, the over-representation of non-European players and the lack of results

[404] Other initiatives include the Cloud Native Computing Foundation (which promotes open-source projects such as Kubernetes and Prometheus) and the CISPE code of conduct on data protection for cloud infrastructure providers.

[405] These documents are the "*Trust Framework- Gaia-X Trust Framework*" (which defines minimum rules for joining the Gaia-X ecosystem in terms of data and infrastructure) (link), the "*Gaia-X - Architecture document*" (which describes the concepts required to establish the Gaia-X ecosystem) (link), the "*Policy rules document*" (which sets out the applicable law) (link) and the "Gaia-X Labelling criteria" (link).

[406] On 17 November 2022, the Gaia-X initiative also unveiled its online platform featuring over 176 cloud services that meet Gaia-X's common rules and standards.

[407] https://www.usine-digitale.fr/article/scaleway-claque-la-porte-du-projet-de-cloud-europeen-gaia-x.N1161587.

[408] Regulation (EU) 2018/1807of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[409] Recital 31 states: "(...)*The codes of conduct should also make clear that vendor lock-in is not an acceptable business practice, should provide for trust-increasing technologies, and should be regularly updated in order to keep pace with technological developments. Throughout the process, the Commission should ensure that all stakeholders are consulted, including associations of small and medium-sized enterprises (SMEs) and startups, as well as users and cloud service providers. It should evaluate the development of these codes of conduct and the effectiveness of their implementation*."

[410] Code of conduct adopted by the SWIPO group on SaaS (link).

[411] Code of conduct adopted by the SWIPO group on IaaS (link).

from this initiative. For example, membership declarations only concern a limited number of services (three services for Amazon out of more than 200, for example)[412].

631. For Cigref, the failure of the cloud market self-regulation process in Europe is essentially the consequence of an asymmetry of skills, resources and objectives between certain major global cloud service providers on the one hand "*who defend the core of their commercial activity and their ability to lock in their customers*", and users on the other "*whose lobbying in this field is not their business*"[413].

632. The Commission's proposal for a Data Act[414] and its impact study[415] confirm the limited effect of the cloud market self-regulation process in Europe, particularly with regard to "SWIPO" codes of conduct on switching cloud service providers. In view of these difficulties, the proposed Data Act aims to harmonise these standards at European level, in particular to encourage migration and interoperability in the sector.

633. In view of the market failures identified, the majority of stakeholders welcome the regulatory initiatives currently underway, in particular the proposed data regulation, which is likely to remove the brakes to migration and interoperability, subject to certain adjustments.

2. THE CURRENTLY EVOLVING REGULATORY FRAMEWORK WILL RESOLVE A NUMBER OF IDENTIFIED OBSTACLES.

a) The Digital Markets Act

634. The DMA represents an important step towards regulating certain practices by gatekeepers, and so helping to restore the smooth running of the internal market. The *Autorité* notes, however, that the provisions of the DMA described above (see Part I) do not appear to address all the competitive risks identified in this opinion.

635. In fact, the implementation of the DMA's obligations and prohibitions is limited, on the one hand, to entities designated as gatekeepers and, on the other, to "essential platform services", provided that these constitute "*a major access point enabling user companies to reach their end users*"[416].

636. Above all, some of the issues identified in this opinion do not seem to be covered by the DMA. For example, situations of lock-in, through trade or technical practices, in which users are prevented from switching to solutions or services that better match their needs, seem to be insufficiently taken into account, as confirmed by some stakeholders. Furthermore, the

[412] https://swipo.eu/current-swipo-code-adherences/ (accessed on 25 June 2023).

[413] https://www.cigref.fr/swipo-echec-regulation-marche-europeen-cloud.

[414] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23 February 2022, page 5;

[415] The European Commission's impact assessment report of 23 February 2022 states, "*The Free flow of non-personal data Regulation introduced a self-regulatory approach to address this problem, by encouraging industrial stakeholders to develop codes of conduct for easier cloud switching. Following a difficult self-regulatory process that missed the regulatory deadline, the resulting 'SWIPO' codes of conduct were presented by mid-2020. Since then, only 16 cloud services of 8 providers have signed up. This is a very small number, considering that one specific provider already offers two hundred different cloud/edge services*" (link).

[416] Articles 5, 6 and 3(1)(b) of the DMA.

question of concrete ways of facilitating provider switching, through standards for example, is not addressed.

637. The DMA does, however, provide for the possibility of the Commission adopting implementing acts to specify the measures that the gatekeeper will be required to implement to comply with the obligations and prohibitions of Article 6. Article 12 also provides for the possibility of updating gatekeepers' obligations following a market survey. However, this option will not be available for several years.

b) The proposed Data Act

638. The draft Data Act has evolved significantly since the Commission's proposal of 23 February 2022. The latest proposal from the Swedish Presidency, available on 12 June 2023[417], includes more significant requirements for certain obligations. Among other things, it clarifies the rights of customers and the obligations of cloud service providers in the event of migration, abolishes migration fees in addition to ending egress fees within three years of the regulation coming into force, and lays down more precise obligations with regard to the technical aspects of switching cloud providers, particularly for PaaS and SaaS services. The conditions for setting standards in the sector have also been clarified.

639. The *Autorité* welcomes this proposal, which is likely to bring about positive changes in the way the sector operates competitively.

640. As the deadline for discussions is the end of June 2023, it is probably not appropriate for the *Autorité* to make proposals to improve the current text. However, in its aforementioned Opinion 23-A-05, the *Autorité* made a number of recommendations to the government concerning certain provisions of the draft law aimed at securing and regulating the digital space, in connection with the provisions of the Data Act relating to egress fees and portability and interoperability obligations. Article 41 of the draft regulation, as amended in the latest proposal from the Swedish Presidency, stipulates that the Commission will evaluate the future regulation within three years of its entry into force and may propose amendments to the European Parliament and the Council if necessary.

641. In this context, the *Autorité* considers it appropriate to submit the following points of vigilance to the parties concerned.

Distinguish egress fees from other migration costs

642. While the current amendments to the draft regulation clearly distinguish between egress fees and other migration fees, they still subject them to the same three-year ban.

643. It should be noted that, in Article 7, II, of the aforementioned draft law to secure and regulate the digital space, the government has proposed to regulate data transfer fees. As indicated in its aforementioned Opinion 23-A-05, while the *Autorité* considers, "*like the Government, that a framework for these fees may be justified to remove the disincentives they may create to migration and multi-cloud architectures*"[418], it also believes that "*the draft law should*

[417] https://www.contexte.com/medias/pdf/medias-documents/2023/6/data-act-8-june-1-b6e578fd381a4fe886cd9c2f6cd52de5.pdf

[418] Opinion 23-A-05, paragraph 77.

reflect the European position, and at the very least provide for the application of a transition period in the gradual elimination of these fees"[419].

644. The costs associated with the work of dedicated teams to support cloud service providers in the change process could be invoiced, which would also improve transparency for the customers concerned.

Carry out an impact study on cloud credits

645. Unlike data transfer fees, there are no plans to regulate cloud credits specifically at European level. In Article 7, III, of the aforementioned draft law to secure and regulate the digital space, the government proposed a framework for their duration and their renewal conditions[420]. In so doing, it wants to ensure that the proposed programmes do not pre-empt or lock-in the market, and can be replicated by smaller providers.

646. The *Autorité* recommends that, as part of the assessment of the future regulation provided for in Article 41, an impact study be carried out on cloud credits, in particular those falling into the category of support programmes (see Part IV.A), to assess their impact and compare their possible effects on competition within the cloud sector with the advantages derived by the companies benefiting from the credits.

Specify measures to promote portability and interoperability

647. As a reminder, Article 23 of the Commission's proposal stipulates that cloud service providers must remove obstacles that could prevent customers from maintaining functional equivalence with "*the same service type*" from a different cloud service provider. Article 26 (1) specifies that IaaS service providers must ensure "*that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service*". In contrast, PaaS and SaaS service providers "*make open interfaces available to the public free of charge*" (emphasis added).

648. Firstly, like several other stakeholders, the *Autorité* wonders about the scope of the notion of "*functional equivalence*" and the way in which it should be ensured (setting up application programming interfaces, opening up source code or publicising documentation). In addition, applying the obligations to maintain functional equivalence only to IaaS services, to the exclusion of PaaS services, seems justified, given the greater homogeneity of IaaS services. The *Autorité* nevertheless identifies a risk that the principle of functional equivalence will affect the freedom to innovate and create new functionalities, and the incentive to do so on the IaaS layer. Some authors fear that these provisions will lead to the establishment of a "*lowest common denominator*" [421]between the cloud services concerned.

649. Secondly, Article 26 (2) of the proposed Data Regulation provides for the provision of "open interfaces" to ensure the interoperability of PaaS and SaaS services. These application programming interfaces, which some stakeholders understand to be open source *i.e.* freely accessible and modifiable, will need to be accompanied by clear, public documentation so

[419] Above-mentioned Opinion 23-A-05, recommendation 4.

[420] Article 7 of the aforementioned draft law to secure and regulate the digital space stipulates that a decree will set "*the conditions to ensure fair competition between cloud computing service providers*", and in particular the duration of cloud credit.

[421] Sean Ennis and Ben Evans, "*Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence*", 29 March 2023 (link).

that third parties can ensure the compatibility of their services. Lastly, it will be important to ensure that companies retain sufficient incentives to continue investing in their upgrades.

650. Thirdly, the proposed data regulation provides for the introduction of standards to facilitate the use of multiple providers (Chapter VIII of the proposed regulation).

651. For reasons of efficiency, standardisation efforts could focus on a limited number of cloud products or services, such as IaaS services. The investigation showed that discussions on the adoption of common standards can be long and difficult. Furthermore, as noted above for functional equivalence, there is a risk that standardisation efforts will lead to limited innovation in the sector, as the cloud products and services concerned will be more homogenous. The quality and safety of these services could also be affected.

652. It would also be advisable to favour non-proprietary solutions where they exist. Standards whose implementation would give rise to intellectual property protection would be likely to raise difficulties. This is not just a theoretical issue, since the question of whether Google had infringed Oracle's copyright by copying Java application programming interfaces for its Android operating system has been the subject of lengthy litigation in the USA[422].

653. Lastly, it is clear from the proposed Data Act that discussions on the development of these standards will be conducted in parallel between industry players and European organisations. It would be advisable to set a deadline by which market players must have adopted a common standard, so as not to slow down the process of adopting standards in the sector.

[422] U.S. Supreme Court decision, Google LLC v. Oracle America, Inc, 5 April 2021. The Court ruled that Google's copying of the API, which included only the lines of code needed to enable developers to put their talents to work on this innovative programme, was a fair use of this content under the law.

Other responses in the event of market failure

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

Indeed, while technical solutions exist to make it easier to switch providers or use multi-cloud (standard services or open-source solutions, for example), self-regulation has not led to the establishment of common technical standards. Incumbent players, particularly hyperscalers, are not necessarily encouraged to develop the best-performing or most cost-effective solutions, as these are likely to erode their market share. Several customers have confirmed that the major cloud service providers are not necessarily looking to offer standard solutions for accessing their cloud services.

In addition, joint initiatives to develop common standards are encountering implementation difficulties, such as Gaia X, initially founded by 22 French and German organisations, and the European SWIPO initiative. Indeed, the presence of hyperscalers in 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 resolving identified market failures, as European regulators have begun to implement in recent months with the DMA and Data Act, or the draft law to secure and regulate the digital space recently presented by the government. In its Opinion 23-A-05 of 20 April 2023 on this draft, the *Autorité*, while sharing most of the concerns met by this draft law, made a number of recommendations designed in particular to ensure that its provisions would be aligned with those of the Data Act.

The opinion also sets out a number of points of concern with regard to the Data Act, in order to strengthen the effectiveness of its provisions. As a result, the costs associated with the work of dedicated teams to support cloud service providers in the change process could be invoiced, which would also improve transparency for the customers concerned. The *Autorité* also recommends that an impact study be carried out on cloud credits as part of the assessment of the future regulation provided for in Article 41. Lastly, the *Autorité* proposes specifying measures to promote portability and interoperability. With regard to this last question, the *Autorité* identifies a risk that the principle of functional equivalence will affect the freedom to innovate and create new functionalities, and the incentive to do so on the IaaS layer. It will also be important to ensure that companies retain sufficient incentives to continue investing in interface upgrades for PaaS and SaaS services. Finally, the *Autorité* proposes focusing standardisation efforts on a limited number of cloud products or services, giving preference to non-proprietary solutions, and setting a deadline by which self-regulation work must be completed.

VII. Perspectives and conclusions

654. The investigation shows that the players anticipate an acceleration in the adoption of cloud services by all companies over the next few years and that there are strong growth prospects for providers of cloud products and/or services.

655. According to the *Autorité*, a number of developments are likely to have an impact on competition in the sector.

656. Firstly, as the *Autorité* has shown (see Part II), the competitive operation of the cloud industry is characterised by competition *for* the market insofar as, for a specific need or workload, customers tend to turn to a single provider, particularly those with an attractive ecosystem. Given the 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. This situation could lead to a reduction in competitive intensity, other than the flow of new customers or new workloads. As a result, the *Autorité* identifies a risk of price increases and/or a drop in the quality of cloud products or services.

657. 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.

658. Firstly, the increasing use of artificial intelligence (hereinafter "AI") will drive growth in demand for cloud services. In fact, the countless developments towards increasingly complex models, such as Large Language Models (hereinafter "LLM") or generative IA, require considerable computing power[423].

659. In addition to OpenAI (creator of ChatGPT and the different versions of GPT: 3, 3.5 and 4), which also has a partnership with Microsoft[424], many players have developed their own LLM technologies, such as Google (LaMDA, Bard) and Meta (BlenderBot3, LLaMA) AWS also recently announced a partnership with HuggingFace[425].

660. The search engine industry seems to be at the forefront of the emergence of LLMs. Microsoft has already announced its intention to associate LLMs with its Bing search engine, and Google wants to do the same with Bard. However, according to some estimates, if Google wanted to associate an LLM response the size of ChatGPT with every search, the level of expenditure could reach $100 billion in infrastructure investments with the current state of technology (graphics processors, servers and connectors)[426]. Although this estimate is deliberately maximalist (as it neglects any future technological gains, in particular), it shows the scale of the expenditure that could be generated by democratising the use of these LLMs.

[423] On these models, the French Center of expertise for digital platform regulation (*Pôle d'expertise de la regulation numérique,* PERen) published a note in April 2023 describing precisely how these algorithms work (link).

[424] Microsoft provides OpenAI with supercomputers to develop its technology, and OpenAI offers its managed products exclusively on Microsoft Azure.

[425] https://huggingface.co/blog/aws-partnership.

[426] https://www.semianalysis.com/p/the-inference-cost-of-search-disruption.

661. In the future, all business sectors will be interested in these technologies, and innovations in artificial intelligence (such as LLMs) will serve as growth drivers for the cloud sector as a whole. Cloud service providers can be mobilised:

- for the provision of managed PaaS services, available to companies whose core business is not AI: this is already the case with the OpenAI services offered on Azure, for example[427];
- for the provision of a sophisticated infrastructure for Tech players wanting to develop AI models (LLM or other). All the major cloud service providers are developing this aspect, such as Google with AI Vertex[428] and AWS with Amazon SageMaker[429].

662. In addition, most players also identify edge computing as an innovation that will have a major impact in the near future. Its development will bring computing and storage closer to the user, for lower latency, lower bandwidth costs, more reliable connectivity and improved security.

663. Other innovations were mentioned by the players interviewed during the investigation[430], such as "ambient compute" or "ambient intelligence", which aims to better integrate information and communication technologies into the everyday environment, by combining the Internet of Things and artificial intelligence technologies[431]. Robotic vacuum cleaners, which use sensors and built-in cameras to determine their trajectories around the home, are a case in point.

664. Some players also hope that future innovations will aim to promote multi-cloud, thanks to improved interoperability at infrastructure and architecture level, and tools to manage these new multi-cloud configurations.

665. The ability of cloud service providers, particularly non-hyperscalers, to embrace these technological challenges could therefore help overcome some of the identified barriers to entry and expansion.

666. Developments in the cloud sector are also likely to be influenced by innovation in security or environmental footprint. As mentioned above, a company like Qarnot Computing, which has just completed a substantial fund-raising round[432], has developed a way of providing computing power with a limited footprint, thanks in particular to the use of the heat emitted by heat-consuming sites (e.g. industrial sites).

667. Lastly, industry players expect the regulatory framework to evolve towards the establishment of new rules, both general and specific, to govern the design, operation, marketing and use of cloud products and/or services.

668. Recent developments in the sector call for vigilance on several levels.

[427] https://azure.microsoft.com/en-in/products/cognitive-services/openai-service/#features.

[428] https://cloud.google.com/blog/products/ai-machine-learning/generative-ai-for-businesses-and-governments?hl=en.

[429] https://aws.amazon.com/fr/blogs/machine-learning/training-large-language-models-on-amazon-sagemaker-best-practices/.

[430] A number of them are interdependent, such as the cloud, edge computing and ambient computing.

Ambient computing: everything you need to know about this IoT cornerstone (link).[431]

[432] Press release, "Qarnot, a specialist in the recovery of IT waste heat, raises 35 million euros to deploy its new-generation data centres", 10 January 2023 (link).

669. It seems crucial that companies make an informed choice of provider, possibly by weighing up the added value of a service against its degree of lock-in[433]. The *Autorité's* investigation has shown that customers generally use a single cloud service provider for each workload, demonstrating the importance of this choice when there are significant barriers to migration and interoperability. These constraints are also expressly recognised by one hyperscaler, who pointed out that "*the more sophisticated the software provided by the cloud, the harder it is to port it to the cloud next door. It is for each customer to decide what they prefer*." Over and above commercial and technical considerations, this implies transparent pricing, so that customers can anticipate the consequences of their choices, and, for customers, retaining the necessary skills in-house and continuing to invest in staff training.

670. The competitive risks set out in this opinion will be carefully analysed by the *Autorité's* departments. If it is not legally possible for the *Autorité* to conduct an investigation into these questions in the context of an opinion, the investigation services may carry out a preliminary examination of the information collected in order to assess whether there are grounds to open one (or more) contentious investigation(s). Only an adversarial examination will establish whether or not these practices are proven, and whether or not they contravene competition law. This vigilance is key to preserving innovation and minimising costs in an industry that represents a major vector of economic growth for companies.

[433] https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud.

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, the competitive operation of the cloud industry is characterised by competition *for* the market more than *in* the market, insofar as, for a specific need or workload, customers tend to turn to a single provider, 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.

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 service 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 impact of the environmental footprint.

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

Deliberated on the oral report by Élodie Vandenhende, Marion Panfili and Laure Dosogne-Varaire, rapporteurs, and the contribution of Yann Guthmann, Head of the Digital Economy Unit, by Benoît Cœuré, President, Irène Luc and Thibaud Vergé, Vice-Presidents.

The hearing secretary,	The Chair,
Habiba Kaïd-Slimane	Benoît Cœuré

APPENDIX - GLOSSARY

To enhance understanding of the opinion, the terms used in it should be interpreted as follows:

- **API:** this term is defined in *Autorité de la concurrence* Opinion 18-A-03 of 6 March 2018 on data mining in the internet advertising sector as "*an acronym for "Applications Programming Interface", i.e. a programming interface that allows two programmes or software to interact with each other, by connecting to exchange data. An API is in principle open and offered by the programme owner. It allows software to use the services and features of other software.*

- **Cloud**: this term is defined by the National Institute of Standards and Technology (NIST) as "*a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*[434]."

- **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, or some combination of them. It exists on the premises of the cloud provider*[435]."

- **Private cloud**: according to NIST, this term refers to products and/or services where "*The cloud infrastructure is provisioned for exclusive use by a single organisation comprising 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*[436]."

- **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*[437]."

- **Dev Ops** combines the words "development" (developers) and "operations" (operational IT teams). The DevOps movement enables closer collaboration between programmers

[434] NIST website.

[435] NIST website.

[436] NIST website.

[437] NIST website.

and the operational teams responsible for deploying and supporting code throughout the product lifecycle.

- **Data**: in the proposal for a data regulation, adopted by the Commission on 23 February 2022, data is defined as: "*any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*".[438]

- **Hyperscalers**: a term for very large companies that have built global hosting capabilities and developed dedicated applicationsused by millions of users.

- **IaaS** *(Infrastructure-as-a-Service*): this term is defined by NIST as "*the capability* (...) *to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls)* [439]".

- **Interoperability**: "*the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data in order to perform their functions*"[440].

- **Multi-*cloud***: a strategy for a company cloud service user to use more than one cloud service provider.

- **PaaS** ("Platform as a Service"): this term is defined by the NIST as "*the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming, languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment*[441].

- **Portability**: "*data portability is the ability to easily transfer data from one cloud service provider to another cloud service provider without being required to export and re-import the data; similarly, application portability is the ability to easily transfer an application or application components from one cloud service to a comparable cloud service and run the application in the target cloud service*".[442]

[438] European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data, Article 2(1) (COM(2022) 68 final, 23 February 2022, page 46;

[439] NIST website.

[440] Definition taken from the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), 23 February 2022.

[441] NIST website.

[442] Study carried out for the European Commission by IDC and Arthur's Legal: "*Switching of Cloud Service Providers*", 8 May 2018, page 3 (link).

- **SaaS** (Software-as-a-Service): this term is defined by NIST as "*The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a programme interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings*[443]."

[443] NIST website.