BoR (24) 52

Draft

BEREC Report on Cloud and Edge Computing Services

7 March 2024

Contents

Executive Summary

Cloud computing underpins most of the developments taking place in the digital sector. Its importance is meant to growth even more in the coming years. Electronic Communication Network and Services (ECN/S) are part of the broad range of services that are evolving thanks to cloudification.

BEREC underlines that the regulatory experience of BEREC's NRAs is particularly valuable to address new emerging issues in the digital sector, including facilitating the development of the cloud and edge services in the European Union (EU). This report aims at shedding further light in the impact of these developments with a particular focus on the electronic communication sector, including a reflection on their regulatory implications. This analysis is meant to contribute to support better informed decisions aimed to reach the political targets for the EU regarding the development of cloud and edge computing, including the objectives in terms of investments and take up set in the EU Digital Decade Policy Programme 2030[1].

Moreover, BEREC acknowledges the role that some of its NRAs are expected to undertake for the implementation of the EU legislation related to cloud and edge services, such as the Data Act. This report could serve as an input for the enforcement of these competences and contribute to a harmonized interpretation of the EU digital framework across the Members States.

With regard to the provision of ECN/S, cloud-based networks not only require new investments to enable new and enhanced services, as in previous network updates, but it also entails a great sectoral transformation and major changes in the value chain. New roles, many times undertaken by new players, are introduced for the provision of ECN/S and new complex competition and cooperation dynamics are taking place among these providers. Furthermore, ECN/S, Information Technology (IT) and cloud/edge computing services, sometimes including other elements such as Artificial Intelligence (AI) systems and Internet of Things (IoT) solutions, are increasingly being provided to the end users by means of fully integrated customized solutions. Overall, all these developments, both regarding the network architecture and the provision of the services to the users, imply that the boundaries between these services blur leading to ECN/S and cloud/edge computing convergence. Those changes are to be closely followed by regulators.

BEREC frames its analysis by taking stock on the definitions and taxonomies of cloud and edge computing services put forward by the EU legislation and standardization bodies.

The risks and challenges faced in the EU for the healthy development of cloud and edge services are outlined. Those challenges relate to the significant additional investment on infrastructures that those services require to flourish; concerns about market concentration

[1] DECISION (EU) 2022/2481 of 14 December 2022 establishing the Digital Decade Policy Programme 2030.

and competition; digital sovereignty; sustainability; users' uptake and development of use cases; interoperability; data protection and cybersecurity.

The EU aims at overcoming these challenges by building a cloud environment with the following characteristics: (i) interconnected (i.e., federated); (ii) interoperable; (iii) trusted; (iv) sustainable and (v) cloud-to-edge enabled (including infrastructures, platforms, marketplaces, services and testing and experimentation facilities for edge AI). In order to advance towards these objectives, the EU has put forward several initiatives and legislations. Among those, BEREC highlights the Digital Decade Policy Program, the European Data Strategy, the Digital Markets Act and the Data Act.

BEREC develops further in the cloud market characteristics building on comprehensive analysis made by NRAs such as ACM and OFCOM and the French NCA. All of them have reached similar conclusions and raised analogous competition concerns regarding concentration in a market featured by economies of scale; ecosystems and network effects: switching and interoperability barriers as well as other constraints to entry and expansion.

In this context and taking into consideration their relevance to foster open and contestable markets, BEREC discusses the EU state of play of interoperability, standards and switching including the barriers faced to switch data processing services and to the use of multi-cloud as well as the consequences that those barriers entail. BEREC welcomes the recent EU initiatives to foster interoperability and standards as well as to facilitate switching by means, in particular, of the Data Act.

The report describes how cloud and electronic communications interplay from four different angles. First, the connectivity required for the provision of cloud and edge computing. Second, the migration of ECN to the cloud considering different elements and functions of the network (core, RAN edge, backhaul and transport as well as network operation and orchestration). Third, the provision of new and enhanced ECN/S by means of cloud-based network services (i.e., Network-as-a-Service). Fourth, supplying of bundled and integrated ECN/S and IT services with cloud.

Against this backdrop, BEREC gathers regulatory considerations around network cloudification.

Namely, BEREC reflects on the definitions and scope of the current European Electronic Communications Code (EECC) in view of the technology developments and convergent trends as well as the need to allow regulation gaining a broader view of the business ecosystems to be able to tackle emerging trends.

Competition implications regarding ECN/S and cloud/edge convergence are approached from four different angles: i) the impact on ECN/S markets; ii) on the cloud markets; iii) the partnerships between ECN/S and cloud providers and vi) the implications of ecosystems including the risk of leveraging market power into adjacent markets.

BEREC points to Application Programmable Interfaces (API) openness as one of the key aspects in the process of ECN/S cloudification. It develops on the consequences of the lack of openness but also on risks, such as discrimination or unfair behaviour, that API exposure might entail if not rightly implemented as well as other challenges related to net neutrality, data privacy and security.

The EECC attributes NRAs and BEREC objectives related to the promotion of efficient investment and innovation in new and enhanced infrastructures while ensuring competition and non-discrimination. In this light, BEREC analyses the conditions and possible obstacles both regarding network upgrades towards cloudification and fostering the connectivity required for edge computing.

BEREC addresses the interplay among the different pieces of EU legislation impacting ECN/S and cloud/edge computing and the need to ensure that those are applied in a coherent and efficient manner avoiding unnecessary red tape for the stakeholders. Also along these lines, the institutional set up should aim at facilitating regulatory enforcement. Regulatory consistency and harmonization should be promoted and coordination among all public bodies involved must be ensured to safeguard the mentioned coherence, providing clear and consistent guidelines to the users and providers, facilitate compliance and allow the necessary regulatory dialogue to enable public enforcers to speak with a single voice fostering legal certainty, regulatory simplification and further efficiency in the enforcement of their policies.

Finally, BEREC acknowledges that other regulatory issues that may arise in this field regarding digital sovereignty, digital divide or environmental impact.

Some future trends are expected to be relevant in the upcoming years. It is foreseeable that the market will continue growing. As IT resources increasingly move to the cloud and the market reaches further maturity, portability, switching and multi-cloud will become increasingly important. Cloud, IT and ECN/S follow a convergent trend. ECN evolve both to adapt to the provision of cloud services and by integrating some of its parts and functions into the cloud. The provision of services tailored to specific customers, integrating Cloud, IT and ECN/S elements, may increase. Partnerships among all players, with diverse and complementary expertise and experience in relation to these different elements will still be required in the mid-term. Among those players, *hyperscalers* are expected to continue holding a central position. Additional efforts on interoperability and seamless computing environments are to continue advancing.

Public consultation questions

This draft report will be subject to **public consultation from 13 March 2024 until 24 April 2024**. Any comments, suggestions, clarifications or further information related to the subject matter are welcomed. Without limiting the scope of the public consultation contributions, BEREC is particularly interested in the stakeholders' views and collaboration regarding the following specific issues:

- Chapter 6.2 develops on electronic communication networks migration to the cloud. One of the preliminary considerations pointed out in this section regards to the scalability constraints that face ECN that might hinder taking fully advantage of network cloudification benefits. It is also argued that mobile networks may face less limitations than fixed networks. Do you agree with these preliminary findings? Please, explain your answer. Are there other scalability constraints to be considered?

- Is there a risk that investments in cloud-based networks crowd out private investments in network coverage and network capillarity? Are investments in network innovation and network coverage substitutes or complements?

- What are your expectations on the evolution of competition in the electronic communication markets given network cloudification? Can market failures in the cloud market affect competition and investment in the provision of electronic communication networks and services? To which extent?

- Are all operators and service providers equally equipped to take advantage of network 'cloudification? What would be needed to ensure that the transition to cloud networks does not create an uneven playing field in electronic communication markets?

- Chapter 7 develops on regulatory considerations related to the different trends described along the report (e.g. the characteristics of the cloud markets, cloud and ECN/S convergence, synergies and dependencies among players and technologies, etc.). Do you agree that those are potential relevant regulatory matters in the coming years? Is there any other potential risk (or opportunities) that regulators should consider?

- What is your opinion on the different hypothetical situations mentioned in Chapter 7.2.2, point vi. "APIs openness and APIs exposure" in which potential issues related to API exposure may arise? Are these hypothetical situations relevant and if so, in what timeframe?

- Technical developments allow for increased connectivity specialization tailored to specific services. From a forward-looking perspective, is there a risk that network capabilities enabled by cloudification, in the context of the observed digital market trends (ecosystems, concentration, network effects, potential for leveraging market power into adjacent markets, etc), could lead to a reconfiguration of the Internet towards separated, proprietary and non-interoperable, environments?

1. Introduction

1.1. Recent evolution of cloud and electronic communications services

In the early 2000s, Information Technology (IT) management evolved towards the centralization of computing resources with the aims to gain computing power, optimizing resources and lower operational expenditure (OPEX) and capital expenditure *(*CAPEX*)*. IT servers of organizations started to be arranged in centralized facilities named *data centres*. The possibility of access to different data centres in different locations gave origin to cloud services as we know them today.

In 2006, Amazon, the current global cloud computing leading company, launched Amazon Web Services (AWS)[2] giving access to third parties to the data centre facilities that had been initially built for the provision of its own services. This new service not only provided a new source of revenues but allowed Amazon to maximize the use of these facilities and further increase scale and scope of its business. The other two main cloud computing providers at this moment, Microsoft and Google, followed in 2008 with Microsoft Azure[3] and Google Cloud[4] respectively. Due to the enormous size reached by these three companies in terms of computation, storage (data centres), network resources and geographic availability, they are commonly known as *hyperscalers*[5].

Pooling IT resources underpins the digitalization of the industry and society, the emergence of new services and permits the development of today's Internet ecosystem as well as expected future developments on Internet of Things (IoT), Artificial Intelligence/Machine Learning (AI/ML), Virtual Reality (VR), etc. Access to highly specialized services is being made affordable and widespread. Users can focus on their core activities while relying on external cloud providers for the provision of IT resources adapted to their needs and complexity, from bare infrastructure services to fully developed software solutions.

Moving resources to the cloud was accompanied by a paradigm shift in the provision of computing services based on the decoupling of hardware and software. Virtual Machines (VM)[6] and containers[7] allow software to become technically more independent or agnostic of the underlying hardware and the isolation of the different processes running on it. Several layers of abstraction or virtualization were required not only for the interoperability of the different IT systems but also for the network connections amongst them. Multi-tenant data

[2] https://press.aboutamazon.com/2006/3/amazon-web-services-launches
[3] https://news.microsoft.com/2008/10/27/microsoft-unveils-windows-azure-at-professional-developers-conference/
[4] http://googleappengine.blogspot.com/2008/04/introducing-google-app-engine-our-new.html
[5] In some cases, Alibaba Cloud is included in the definition. However, due to its lower footprint in Europe at this moment, the current report considers mainly Amazon, Microsoft and Google under this term.
[6] A VM is a software that emulates a physical computer. Several VM with different Operating Systems (OS) can run on the same hardware, managed by a piece of software named *hypervisor*.
[7] A container allows different apps on the same OS to run on an isolated environment without interfering each other.

centres require a separate connectivity to keep VM and containers isolated. This is achieved thanks to network virtualization techniques that provide for a virtual, or overlay, network over the physical infrastructure allowing a logical separation of the communication.

Network virtualization is also being applied beyond data centres by electronic communication providers. IT and electronic communications have evolved together towards the virtualization of IT resources and network functions that were previously provided by means of IT hardware and network physical equipment. As described in Chapter 6, dedicated physical equipment is being more and more substituted by software solutions in virtualized environments for the provision of electronic communication services (ECS) leading to even further convergence of IT and electronic communications.

The transition to cloud-based networks is meant to entail a great sectoral transformation similarly to major past transitions such as the move from traditional voice-oriented networks to broadband-based networks offering Internet based services. Changes not only require network investment and adaptation by operators as previous network updates, but they also bring new players into the provision of the services that may eventually have a central role. Ultimately, markets could face a complete reshaping that regulators will have to follow and understand.

Furthermore, cloud and electronic communication networks and services (ECN/S) providers are increasingly intertwined in a double direction client/supplier relationship. On one hand, connectivity is required for the provision of cloud computing, both for communication among data centres and with the users. On the other hand, network virtualization (in particular, for 5G services[8]) leads to the use of cloud native solutions as well as an increased interest on software capabilities. Ultimately, the boundaries between ECN/S and cloud computing blur. This trend is meant to be exacerbated as new edge computing services and network as a service (NaaS) solutions enter the market.

Additionally, business users' demand for customized solutions integrating cloud and ECN/S is significantly increasing, as pointed out by a recent BEREC's external 'Study on Communication Services for Businesses in Europe: Status Quo and Future Trends'[9]. In order to provide these services, cloud and ECN/S providers reach partnerships to cover all the elements required by the users.

As further explained in Chapter 4, the provision of cloud services features significant sunk costs, economies of scale and scope, and ecosystem effects. Those characteristics entail barriers to entry that, ultimately, raise competition concerns. Cloud services are provided in a

[8]BEREC Report on the 5G Ecosystem extensively develops on this. BoR (22) 144 https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-5g-ecosystem
Along the same lines, the 5G PPP Technology Board has signaled the role of edge computing to enhance 5G value proposition and its impact in network design. Edge Computing for 5G Networks (2021).

[9] BEREC External Study on Communication Services for Businesses in Europe: Status Quo and Future Trends BoR (22) 184 https://www.berec.europa.eu/en/document-categories/berec/others/external-study-on-communication-services-for-businesses-in-europe-status-quo-and-future-trends

highly concentrated market, where hyperscalers play a central role thanks not only to their size but also to the existence of network and ecosystem effects that can potentially lead to the possibility to leverage market power from adjacent markets.

The global data volume is growing very fast. Whereas cloud computing happens mostly in large data centres today, according to the European Commission (EC)[10], by 2025 this trend will reverse: 80% of all data is expected to be processed in smart devices closer to the user, known as edge computing. The availability of both edge and cloud computing is essential in a computing continuum to ensure that data is processed in the most efficient manner. Energy-efficient and trustworthy edge and cloud infrastructures will be fundamental for the sustainable use of these technologies.

In addition to market concentration, the development of European Union (EU) data processing services faces other challenges related to the investment requirements, contestability, cybersecurity, sustainability or digital sovereignty. Against this backdrop, the EU institutions have put forward a number of initiatives and regulations, such as the NIS 2 Directive[11], Cybersecurity Act[12], the Digital Markets Act[13] (DMA), the Data Act[14] (DA) or the proposal for an Artificial Intelligence Act (AIA)[15] to overcome those and foster the construction of a European federated data space, interconnected and interoperable. Chapter 3 develops on these matters.

1.2. Scope and objectives of the report

The European competitiveness and capacity of innovation strongly depend, now and in the years to come, on the availability of infrastructures and the good functioning of data processing services and connectivity. BEREC acknowledges the importance of these services in the digital economy and fully shares the political targets for the EU in this field. BEREC aims to contribute and cooperate with the rest of the European institutions to fulfil these EU goals.

A number of ECN/S NRAs are expected to have an enforcing role in the implementation of the EU legislation related to cloud and edge services. For instance, the DA requires that the enforcement of some of its provisions is done by national authorities with experience in the field of data and electronic communications. This report could serve as an input to facilitate the informed enforcement of these competences and contribute to a harmonized interpretation of the EU digital framework across the Members States.

---

[10] https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

[11] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) https://eur-lex.europa.eu/eli/dir/2022/2555

[12] Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/eli/reg/2019/881/oj

[13] http://data.europa.eu/eli/reg/2022/1925/oj

[14] http://data.europa.eu/eli/reg/2023/2854/oj

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

Furthermore, the provision of cloud and edge services and ECN/S is increasingly interrelated. Such trend has significant implications. At a technical level, it will allow efficiency gains and the emergence of new services. From a market perspective, it will entail new dynamics and, potentially, shifts in the market relations, roles and positions in the value chain of the different players. From a regulatory perspective, it implies the need to ensure the coherent and efficient implementation of the different EU Acts impacting both ECN/S and cloud services. This interrelation entails that any development or regulation in the cloud sector will impact the electronic communications sector and vice versa. In this regard, this report reflects on the possible regulatory considerations related to network cloudification in Chapter 7.

BEREC acknowledges that the regulatory experience of BEREC's NRAs is particularly valuable to address new emerging issues in the digital sector, including facilitating the development of the cloud and edge services in the EU. The main concerns shared by some players regarding cloud services (e.g., market concentration, sunk costs, barriers to switching, lack of sufficient transparency toward the users, etc.) have been successfully addressed by NRAs for ECN/S. In this context, the present report seeks to gain further knowledge of the state of play of cloud and edge services and understand their interplay with ECN/S including competition/cooperation dynamics. It allows continuing BEREC's open and constructive dialogue on this matter with all relevant stakeholders.

To deliver this report, BEREC carried out an extensive desk research and interviews with OFCOM and relevant stakeholders listed in ANNEX III. The report builds as well on the following BEREC's previous and related work:

i. BEREC input to the EC's exploratory consultation on the future of the electronics communications sector and its infrastructure[16]
ii. Input paper on Potential Regulatory Implications of Software-Defined Networking and Network Functions Virtualisation[17];
iii. Workshop on Open RAN[18];
iv. Report on the Data Economy[19];
v. Report on the Internet Ecosystem[20];
vi. Report on the 5G Ecosystem[21];
vii. Statement on the draft Data Act[22];
viii. High-Level Opinion on the European Commission's proposal for a Data Act[23];

[16] https://www.berec.europa.eu/en/document-categories/berec/others/berec-input-to-the-ecs-exploratory-consultation-on-the-future-of-the-electronics-communications-sector-and-its-infrastructure
[17] https://www.berec.europa.eu/en/document-categories/berec/others/input-paper-on-potential-regulatory-implications-of-software-defined-networking-and-network-functions-virtualisation
[18] https://www.berec.europa.eu/en/events/berec-events-2022/berec-workshop-on-open-ran
[19] https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-data-economy
[20] https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem
[21] https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-5g-ecosystem
[22] https://www.berec.europa.eu/en/document-categories/berec/others/berecs-statement-on-the-draft-data-act
[23] https://www.berec.europa.eu/system/files/2022-07/BoR%20%2822%29%20118_BEREC%20H-L%20Opinion%20on%20the%20ECs%20proposal%20for%20a%20Data%20Act_0.pdf

ix. Workshop on Switching and Interoperability of Data Processing Services[24];
x. BEREC External study on the trends and policy/regulatory challenges of cloudification, virtualisation and softwarisation in telecommunications (hereinafter, the External Study)[25];
xi. BEREC Report on the entry of large content and application providers into the markets for electronic communications networks and services[26].

In the last quarter of 2024, BEREC will further explore how the technological developments, including cloudification and softwarisation, could impact the security of the networks and services in Europe, and how BEREC could contribute to mitigating the risks associated with these developments by means of an external workshop[27].

2. Cloud and edge services: definitions and taxonomies

2.1. Definitions

2.1.1. Cloud services

Cloud services refer to computing resources and applications delivered over the internet. These services are typically hosted by third-party providers and can be accessed by users from anywhere with an internet connection.

The US National Institute of Standards and Technology (NIST) has identified five essential characteristics of cloud services[28]: (i) on-demand self-service; (ii) broad network access; (iii) resource pooling (vi) rapid elasticity and (v) measured service[29].

Those characteristics imply that the user can adapt the consumption of computing services automatically (i.e., without human interaction with the provider), the capabilities required by the user at each time are elastically provisioned, under on a “pay as you go” basis and the user access those capabilities over the network from any location and from many different devices and platforms. The providers pool the resources to serve multiple consumers using a

[24] Summary report https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-data-act-workshop-workshop-on-switching-and-interoperability-of-data-processing-services
Workshop documents and video https://www.berec.europa.eu/en/events/berec-events-2023/berec-workshop-on-switching-and-interoperability-of-data-processing-services
[25] External study on the trends and cloudification, virtualization, and *softwarization* in telecommunications BoR (23) 208 https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-trends-and-cloudification-virtualization-and-softwarization-in-telecommunications
[26] https://berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-entry-of-large-content-and-application-providers-into-the-markets-for-electronic-communications-networks-and-services
[27] BEREC Work Programme 2024. BoR (23) 210 https://www.berec.europa.eu/en/document-categories/berec/berec-strategies-and-work-programmes/berec-work-programme-2024
[28] NIST SP 800-145. The NIST Definition of Cloud Computing https://doi.org/10.6028/NIST.SP.800-145
[29] It is noted, however, that, in the case of private networks, elasticity or the measured services characteristics are not always fully met.

multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

The EU legal definition of cloud computing services is included in NIS 2 Directive on measures for a high common level of cybersecurity across the Union. This Directive defines cloud computing service as *a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations*. The DMA refers to this definition.

Some cloud services fall also under the definition of article 2 of the EECC and, thus, are at the same time ECN/S. Consequently, these particular services need to comply with the electronic communications' regulatory framework. Some examples include (as defined by the ITU[30]) Communications as a Service (real-time interaction and collaboration[31]); Network as a Service – NaaS - (transport connectivity and related network capabilities); Email as a Service (email service including related support services such as storing, receiving, transmitting, backing up and restoring email).

2.1.2. Edge computing

As outlined in the previous Chapter, cloud services emerged as centralization of IT resources. With the time, new use cases and enhanced services are emerging leading the sector towards decentralization by means of edge computing.

The EU defined edge nodes in the EU Digital Decade Policy Programme 2030[32] as distributed *data-processing capacity connected to the network and located close to or in the physical endpoint where the data is generated, which offers distributed computing and storage capabilities for low latency data processing*.

While cloud services are delivered from centralized data centres, edge services are delivered from distributed computing resources. The edge computing infrastructure typically consists of small-scale data centres, servers, and other computing devices that are distributed across the network edge. The location of the edge depends on the use case and application and is typically determined by factors such as the network topology, the amount of data generated, and the latency requirements of the application. For example, the edge could be a local server located in a factory, a mobile device, or a smart city infrastructure.

[30] Recommandation ITU-T Y.3500. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3500-201408-I!!PDF-E&type=items

[31] For example, interpersonal communication services based on numbering provided by cloud service providers (e.g., Amazon Connect, Google Voice), as well as those independent of numbering (e.g., Microsoft Teams), are considered electronic communication services according to the Electronic Communications Code.

[32] DECISION (EU) 2022/2481 of 14 December 2022 establishing the Digital Decade Policy Programme 2030.

Edge computing provides a number of advantages:

i. Decreases latency regarding the provision of services in the cloud (see Figure 1*Figure 1*)
ii. Reduces network traffic. For example, instead of sending back and forward to the data centre to be processed, the data generated by an IoT device, that can be very large, can be aggregated (and analysed/processed) at the edge and send only processed data to the cloud. Ultimately, it entails lower costs and energy consumption reducing the environmental impact.
iii. Allows further control of the location of the data (relevant for privacy or regulatory compliance) as edge computing enables data processing, storage, and analysis at the source where the data is generated.
iv. Enhances the resilience of the network.
v. Allows the possibility of autonomous operation of devices.

There are strong synergies between edge computing and 5G Standalone (5G SA), enabling both a range of critical low-latency applications, leading to emerging applications and use cases. In general, applications that require low latency, communication reliability, and high bandwidth can be more efficiently provided with edge computing resources. Edge computing is particularly well-suited for services such as vehicle-to-everything (V2X) communication, augmented reality applications, real-time video analysis, location-based services, or optimized local content distribution for both consumers and vertical industries.

Further synergies are found among AI, 5G, IoT and cloud/edge services. AI systems support the automation of network functions[33] for cloud-based networks. In turn, some AI systems would require the capabilities provided by 5G and edge computing. Along these lines, the 'Study on the Economic Potential of Far Edge Computing in the Future Smart Internet of Things'[34] identifies the convergence between edge AI and 5G as one key driver for the short / mid-term development of IoT services and point to the use of AI & ML at the edge as one of the most important innovations for the digital transformation.

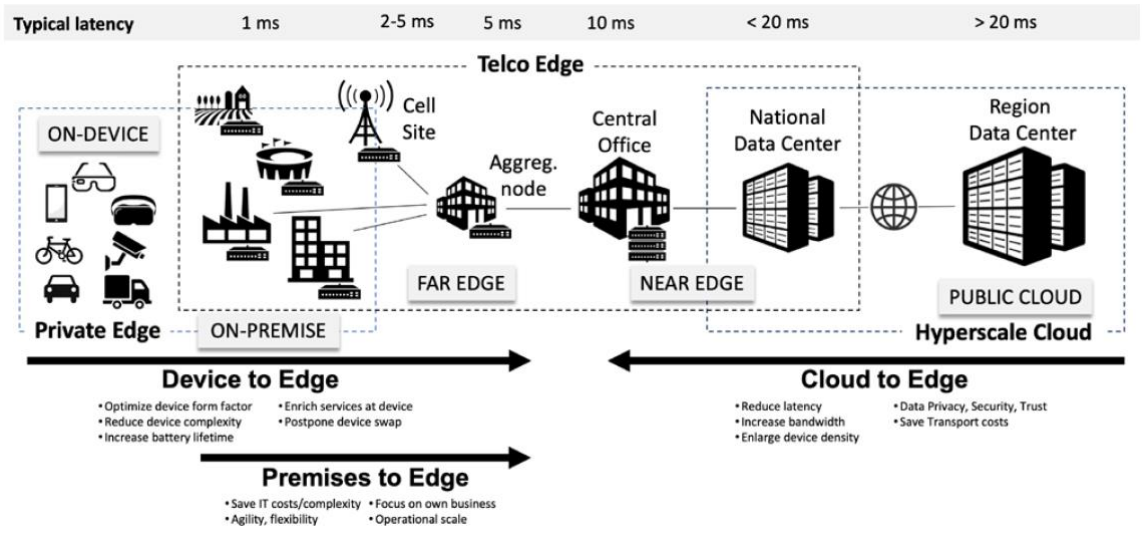
The EC has estimated that, by 2025, 80% of the generated data will be processed at the edge[35]. This edge infrastructure will rely on high quality connectivity to ensure the effective provision of the services with sufficient quality of experience (QoE).

[33] Further insights on the role of AI in telecommunication networks and services can be found in the BEREC Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation. https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-impact-of-artificial-intelligence-ai-solutions-in-the-telecommunications-sector-on-regulation

[34] European Commission, Directorate-General for Communications Networks, Content and Technology, Saint-Martin, L., Delesse, J., Tual, J. et al., Study on the economic potential of far edge computing in the future smart Internet of Things – Abstract, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2759/189170

[35] https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

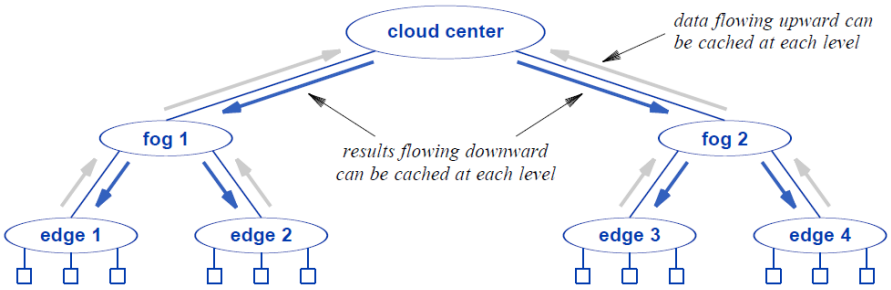
Figure 1 Scope of Telco Edge and drivers to use it.



Source: GSMA. Telco Edge Cloud Value & Achievements Whitepaper. March 2022[36]

Cloud decentralization permits as well "data caching" at different levels. That means that each level keeps a copy of the data generated and flowed upwards. In the example captured in Figure 2, each of the edges would keep a local copy of the data, the intermediate data centre fog 1 would cache a copy of edge 1 and 2 and the cloud data centre of all the edges. Caching allows reducing latency keeping data nearer the source and making it available when required. It is also an example of how cloud and edge interrelate and complement each other.

Figure 2 Basic example of decentralized architecture for data caching.



Source: The Cloud Computing Book: The Future of Computing Explained. Douglas Comer. 2021

[36] https://www.gsma.com/futurenetworks/wp-content/uploads/2022/03/GSMA-TEC-Value-Whitepaper-v13.pdf

2.1.3. Data processing services

The recent DA lays down the concept of data processing services. According to the DA, 'data processing service' means a *digital service enabling ubiquitous, and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature, provided to a customer, that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

That is, the DA aims at a broader sense by including explicitly cloud and edge aspects in their scope. The definition aims at being future proof encompassing cloud, edge as well as other services that may emerge (e.g., fog computing).

The data processing definition in the DA builds and updates the characteristics identified in 2011 by the NIST and develops on the interpretation of the different elements of the definition (scalable, shareable, distributed…) in recitals 80 and 81.

2.2. Taxonomies

2.2.1. Cloud Computing Stacks

The most commonly used taxonomy of cloud services is based on the capabilities provided to the customer. In this regard, cloud services can be broadly categorized into three main service models[37]:

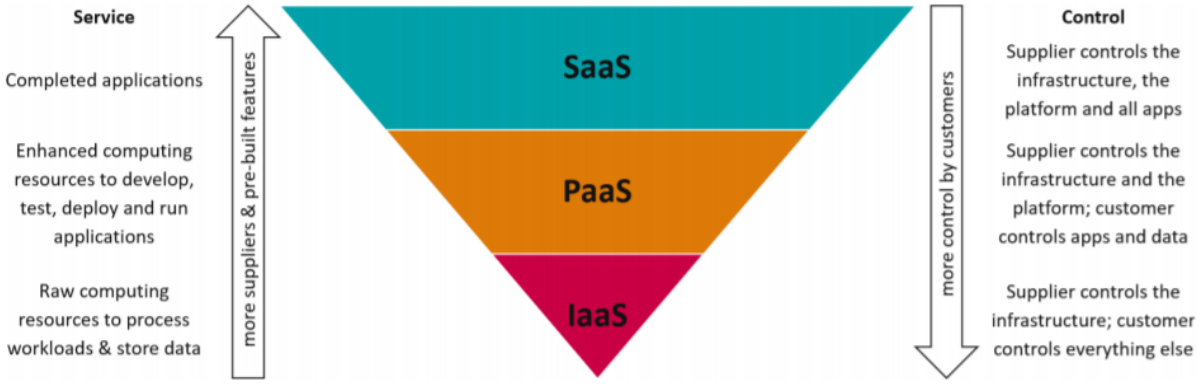
i. **Infrastructure as a Service (IaaS):** refers to the delivery of computing infrastructure. The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. This allows users to access computing resources without having to invest in physical hardware.

ii. **Platform as a Service (PaaS):** provides a platform for developers in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider, without having to manage the underlying infrastructure.

iii. **Software as a Service (SaaS):** provides access to pre-built software applications that are hosted by the cloud provider and accessed by users over the internet.

[37] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST), September 2011; https://www.acm.nl/en/publications/market-study-cloud-services ACM Market Study Cloud Services.

Figure 3 The Cloud Computing Stack



Source: Ofcom[38]

2.3. Cloud Deployment Models

Cloud deployment models represent how cloud computing can be organized based on the control and sharing of physical or virtual resources. The ITU has categorized the following cloud deployment models[39]:

i. **Public cloud:** cloud resources and services are provided by third-party cloud providers over the internet. Public clouds have very broad boundaries, where cloud service customer access to public cloud services has few, if any, restrictions.

ii. **Private cloud:** cloud resources and services are dedicated to a single organization. It can be hosted in a private data centre or managed by a third party. Private clouds seek to set a narrowly controlled boundary around the private cloud based on limiting the customers to a single organization.

iii. **Hybrid cloud:** A hybrid cloud is a cloud deployment model that combines elements of both public and private clouds.

The ITU also points to the different incentives that users have to choose one deployment model over the other. The public cloud allows further cost-effectiveness through pay-as-you-go pricing, scalability to easily adjust resources, and a global network of data centres for high availability and low-latency access, all while benefiting from managed services, security, and an extensive ecosystem of tools and integrations. On the other hand, private cloud provides

[38] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/256457/cloud-services-market-study-interim-report.pdf page 20.

[39] https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-Y.3500-201408-I!!PDF-E&type=items The ITU model includes the additional category of "community cloud" referring to cloud services that are shared by a specific group of customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. This model is not currently as widespread used as the other three.

enhanced security (as the infrastructure is not shared) and data control, customization to meet specific business needs, and the ability to comply with strict regulatory requirements. Hybrid models permit the user benefiting from both models by running some workloads and applications in a private cloud environment while utilizing the public cloud for others. On the other hand, hybrid clouds face their own complexities and security risks[40].

An important point to consider is that private clouds don't always meet all the characteristics associated to cloud services as they don't enjoy the same degree of scalability as public cloud[41] and are not typically billed on a pay per use basis. Along these lines, these services may not meet all the characteristics to fall into the above-mentioned EU legal definitions of cloud and data processing services when they are not scalable or shareable.

In addition to the decision of adoption of a public, private or hybrid model, the user can also opt for a multi-cloud[42] deployment strategy. That solution involves using multiple cloud service providers to host various parts of an organization's infrastructure or applications.

The multi-cloud approach can offer advantages such as reducing vendor lock-in, optimizing costs by choosing the best services from different providers, enhancing redundancy and disaster recovery, improving infrastructure geographic footprint and performances (e.g. latency), and tailoring cloud solutions to specific business needs, ultimately increasing flexibility and resilience in the cloud ecosystem.

On the other hand, multi-cloud solutions can be hindered by the lack of interoperability of the different workloads run in different cloud environments and the difficulties to make use of the data from one cloud to the other. These barriers, that the DA aims to address, are further analysed in Chapter 5.

3. Cloud and edge services in the EU

3.1. Challenges

Both cloud and edge computing services are meant to become critical for many businesses across the economy, including ECN/S operators, broadcasters and public sector organisations. Cloud and edge computing services can enable the development of innovative applications that have the potential to improve the quality of life of the citizens, support economic growth and enhance the competitiveness of businesses. Therefore, the EU

[40] Among those, the following security risk in hybrid cloud environments are noted: i) increased attack surface; ii) increased complexity in managing security (managing security across different platforms, each with its own security policies, configurations, and tools making it challenging to maintain consistent security posture and prevent misconfigurations that could lead to vulnerabilities) and the iii) shared of security responsibilities between the organization and the cloud provider.

[41] The scalability in private clouds is limited by the available physical infrastructure.

[42] Operationalizing Multi-Cloud Environments Technologies, Tools and Use Cases. 2022. https://link.springer.com/book/10.1007/978-3-030-74402-1

economic competitiveness relies on the provision of the services in healthy and trusted markets. A number of challenges that may hinder the development of data processing services in the EU are summarized in Table 1.

Table 1 Challenges to the development of data processing services in the EU

Investment	Significant investment on infrastructures, both in connectivity, (flexible architectures - by using SDN and NFV technologies) and data processing services, are required[43].
Competition concerns	Market concentration, together with existing barriers to interoperability and switching have raised competition concerns[44].
Skilled workforce	The development of EU data processing services requires a skilled workforce and very specialized expertise[45].

[43] According to the 2030 Digital Compass, "*many of the future data services and 5G applications, (…) require a latency of a few milliseconds. To achieve such a latency in return requires an edge node in every 100km".* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0118

[44] See Chapter 4.

[45] According to the feedback received from stakeholders this is currently a scarce resource insufficient to meet the market needs. Similar concerns regarding the lack of skilled workforce in the EU have been acknowledged in the 2023 Chips Act https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1781

Digital Sovereignty	The European strategy for data[46] states that the low share of EU cloud providers not only entails competitive disadvantages for the EU digital sector but also the dependence on external providers that raise vulnerability concerns regarding data threats.
Sustainability	Although data processing services and connectivity facilitate the provision of more sustainable services, their consumption of resources (such as energy and water) implies a significant environmental footprint.
Uptake & development of use cases	According to Eurostat[47], cloud computing is yet to go mainstream for businesses along the EU. 41% of EU enterprises used cloud computing in 2021, mostly for e-mail and storage of files. Additionally, in the case of edge computing, currently there is only a small number of commercially viable use cases in need of more comprehensive latency requirements than provided by current infrastructure resulting in little demand. Innovation, competitive markets and low barriers to entry are key to enable conditions for companies to create new products and technologies.
Interoperability	Lock-in strategies are seen as one of the main constrains for the development of mature tailored cloud and edge computing solutions. Those could drive fragmentation of the cloud infrastructure layer for ECN/S and edge services, which effectively imply a limited and restricted offer to the users and difficulties for them to switch providers.

[46] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066
[47] https://ec.europa.eu/eurostat/statistics-explained/index.php

Cybersecurity	The use of cloud and edge computing services require tailored cybersecurity measures. Likewise, the increasing usage of virtualization in the implementation of cloud infrastructure adds a layer of complexity between the operating system and the underlying hardware that needs to be managed and tackled in terms of security. Moreover, cloud and edge services imply the delegation of business' processing and storage of data to third parties leading to certain risks associated to the transmission and data entrustment in terms of security and privacy[48].

3.2. EU Policies and regulations

Since 2012, the EU has worked to overcome these challenges by building a cloud environment with the following characteristics: (i) interconnected (i.e., federated); (ii) interoperable; (iii) trusted; (iv) sustainable and (v) cloud-to-edge enabled (including infrastructures, platforms, marketplaces, services and testing and experimentation facilities for edge AI).

Therefore, the ambition of the EU is the construction of European federated data spaces, interconnected and interoperable, where services are available on a common European cloud services marketplace. A non-exhaustive overview of the EU initiatives to achieve these goals is gathered in ANNEX I. The most relevant ones for the scope of this report are further described in this chapter.

3.2.1. Digital Decade Policy Program

The Decision establishing the Digital Decade Policy Programme 2030 sets out a series of general objectives and targets to guide Europe's digital transformation in this decade. One of these general objectives is *"developing a comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity work in convergence, to promote their uptake by businesses in the Union, and to create opportunities for growth and jobs through research, development and innovation, and ensuring that the Union has a competitive, secure and sustainable data cloud infrastructure in place, with high security and privacy standards and complying with the Union data protection rules"*. This ambition is anchored in two concrete objectives for 2030: i) 75% of European businesses should use cloud-edge technologies for their activities and ii) the deployment of 10,000 climate-neutral and highly secure edge nodes will provide the necessary connectivity and enable rapid data transfers.

[48] According to the Cloud Security Alliance, the top three threats to cloud systems are: unsafe API interfaces, data loss or theft and hardware failure. ENISA has recently published the Cloud Cyber Security Market Analysis were the basis of the trends in the market are analysed both from the demand and supply sides. https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis

3.2.2. European Data Strategy

The EC has qualified data as the “lifeblood of economic development”, being an essential resource for the provision and creation of digital services across all economic sectors. The actions proposed in the EU Data Strategy aim to facilitate the move to the edge, while developing interoperable cloud and edge services to support the building of common European data spaces[49].

3.2.3. Digital Markets Act

The DMA includes in its scope cloud computing services as one of the Core Platform Services (CPSs) potentially subject to regulation in case that a provider meets the criteria laid down in the Act to be designated as gatekeeper. In that case, a number of obligations would have to be fulfilled by such provider. These obligations are not specific to cloud services and not all of them are in practice applicable to those. Among the ones that would be, in principle, suitable for cloud services, the DMA includes several provisions aimed for increasing data portability and interoperability. Nevertheless, at the moment of drafting this report, no gatekeepers for cloud computing services have been designated and, thus, the DMA is not currently being applied to any cloud service.

3.2.4. Data Act

The DA aims to improve the conditions under which businesses and consumers use cloud and edge services in the EU[50], and support cloud adoption in Europe, which in turn stimulates efficient data sharing within and across sectors. Additionally, the DA sets governance and implementation rules for the enforcement of these obligations. Member States will designate or establish independent competent authorities responsible for the application of the Regulation following certain requirements. In the case of switching obligations, the national competent authority shall have experience in the field of data and electronic communication services.

---

[49] Among the actions contributing to reach these objectives, the EU has foreseen i) public funding for Important Project of Common European Interest (IPCEI) to federate energy-efficient and trustworthy cloud infrastructures and related services; ii) the development of SIMPL, an open source, sustainable and secure middleware that will enable cloud-to-edge federations and be the core software powering Data Spaces otherwise funded by the EU; iii) the EU Cloud Rulebook to provide a single European framework relevant binding and non-binding rules for cloud service users and providers in Europe and iv) Guidance on public procurement of data processing services including recommendations for implementing consistent national policies complemented by a comprehensive set of essential criteria for data processing services to be considered by public sector bodies during the tendering process.

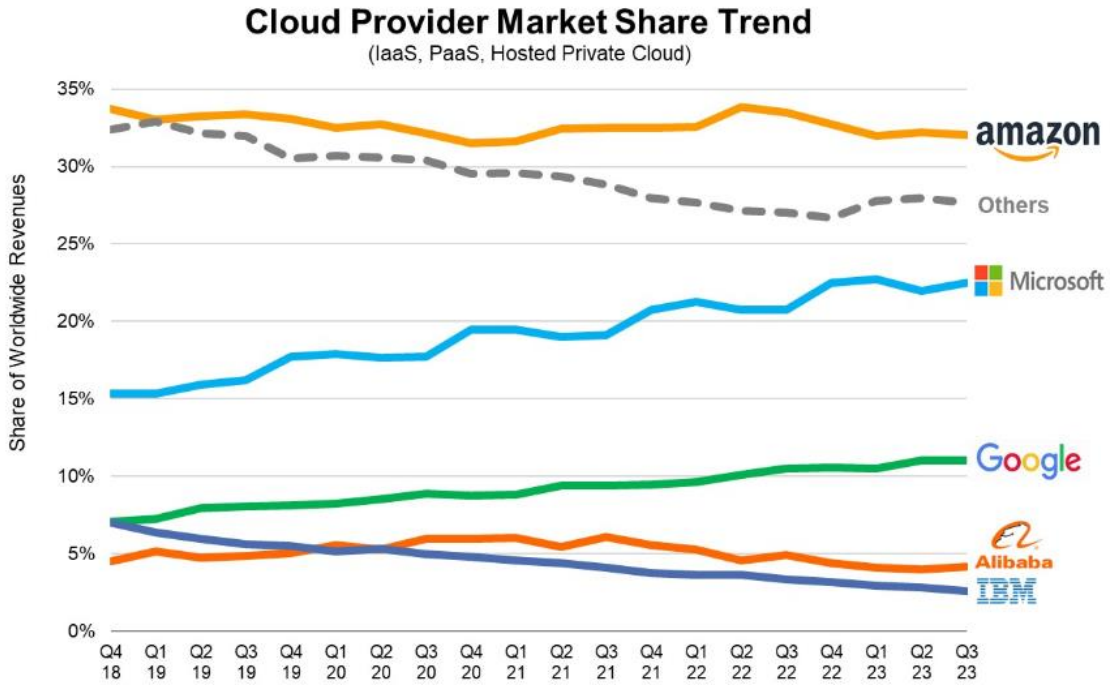
[50] The DA will facilitate moving data and applications (from private photo archives to entire business administrations) from one provider to another without incurring any switching charges, because of new contractual obligations for cloud providers and a new standardisation framework for data and cloud interoperability and to facilitate switching. In addition, the DA will raise trust by introducing mandatory safeguards to protect data held on cloud infrastructures in the EU. This will avoid unlawful access by non-EU/EEA governments.

4. Cloud Market characteristics

The provision of cloud services requires significant investments in infrastructures, such as data centres and connectivity, as well as on IT resources and specialized staff[51]. The sector features significant sunk costs, scale and scope economies and ecosystem effects. Those characteristics entail barriers to entry that, ultimately, raise competition concerns.

The sector is in a period of growth and expansion. Users are moving workloads and data to the cloud as well as acquiring new cloud-based services they weren't using before. The Synergy Research Group[52] reports an increase of global cloud spending in Q3/2023 of over $10.5 billion from 2022. However, this growth has been mainly capitalized by the *hyperscalers*, with a collective worldwide market share of 66%.

Figure 4 Cloud services worldwide market shares



Source: Synergy Research Group

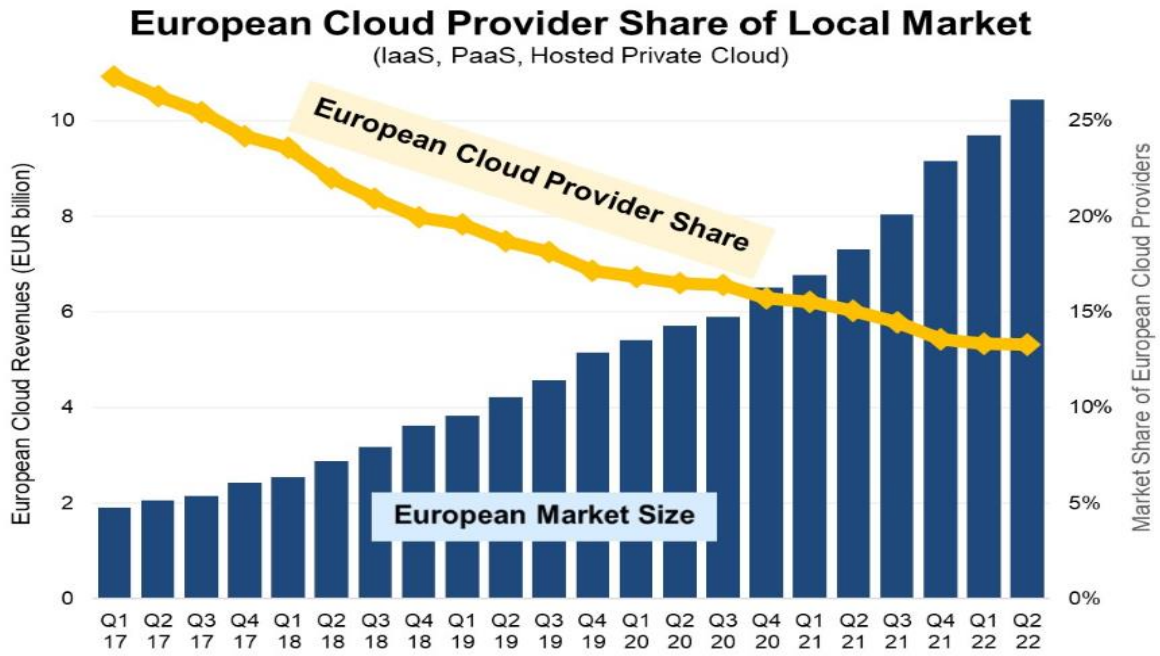
In Europe, the Synergy Research Group[53] indicates that *hyperscalers* account for 72% of the regional market and their share continues to steadily rise while European providers' market share is decreasing despite of the growth of the European market.

[51] During the informal interviews carried by BEREC with the stakeholders (see ANNEX III), it was pointed out that specialized staff on cloud services is currently a very scarce resource.

[52] https://www.srgresearch.com/articles/q1-cloud-spending-grows-by-over-10-billion-from-2022-the-big-three-account-for-65-of-the-total

[53] https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share

Figure 5 EU cloud services market shares



Source: Synergy Research Group

A 2021 KPMG Report[54] foresees that the size of the EU cloud and electronic communications markets will be equivalent in 2027 and compares the regulatory environment for electronic communication services (closely monitored by regulatory expert bodies such as NRA and BEREC) with the lighter regulation on cloud services.

Against this backdrop, several recent comprehensive analyses made by NRAs such as ACM[55] and OFCOM[56] and the French NCA[57] indicate that the cloud services market is highly concentrated and raised concerns about the current competition dynamics. More concretely, these studies identify the following characteristics of cloud markets:

i. Economies of Scale

The market structure is to a large extent the consequence of the prevalent economies of scale. Data centres are very expensive to install with high costs for servers, infrastructure and cooling equipment (high CAPEX), but are also very expensive to run (high OPEX). The ACM study

[54] https://kpmg.com/fr/fr/home/insights/2021/04/cloud-europeen-croissance-enjeux.html

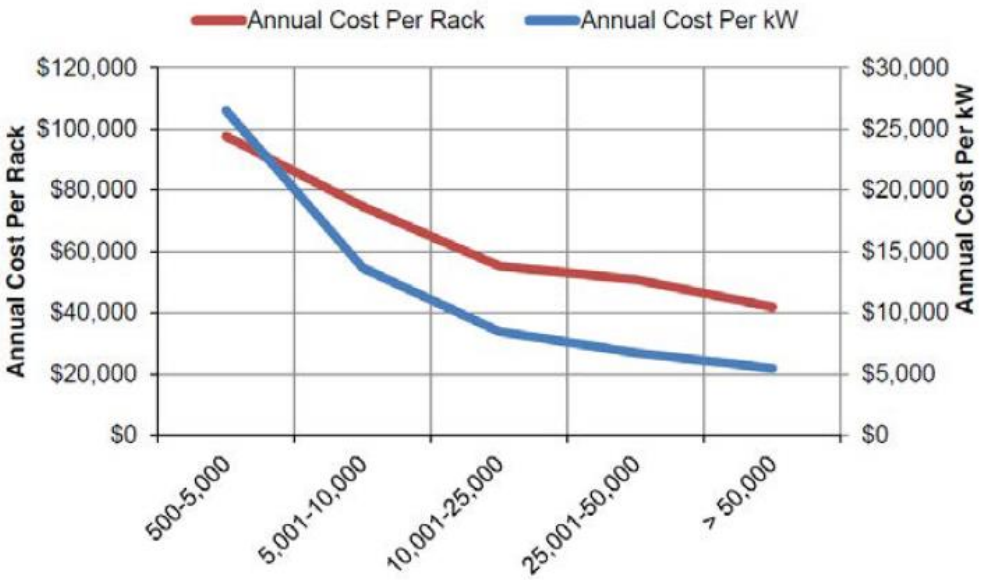
[55] ACM Market Study Cloud services https://www.acm.nl/system/files/documents/market-study-def-public.pdf or

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

[57] Autorité de la Concurrence Avis 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage ("cloud") https://www.autoritedelaconcurrence.fr/fr/avis/portant-sur-le-fonctionnement-concurrentiel-de-linformatique-en-nuage-cloud

mentions operational costs and energy costs as the main responsible factors for the economies of scale, as depicted in Figure 6, but all other costs factors contribute as well.

Figure 6 Cloud operational and energy costs



Source: ACM

The prevalent economies of scale have a self-enhancing effect. One multiplier effect is that larger data centres, with more clients are less subject to variance of usage and thereby can make better scalability offers. The hyperscalers have a global presence with their data centres, which contributes to their competitiveness.

Companies with a very high internal supply of cloud services thereby have an advantage over other cloud providers. Microsoft, Google and Amazon have so many web-based services that their cloud size automatically comes in the larger scales.

ii. Ecosystems and network effects

Hyperscalers provide the full cloud computing stack, and also host PaaS and SaaS products, sometimes developed by independent software vendors (ISVs) and offered in the hyperscaler's marketplace. A hyperscaler, often in a partnership with ISVs, are able to offer hundreds of services.

The technology, software, and APIs of the cloud providers can differ. This makes it more difficult for ISVs to develop services that can be used by different cloud providers. Since the development of these services costs time and resources, the ISVs only typically develop services for one or a few cloud providers, notably the bigger ones, the hyperscalers. Cloud providers with the most customers attract the most ISVs. As mentioned above, this creates ecosystems around a few cloud providers i.e., hyperscalers reinforcing network effects.

Other competition concerns related to ecosystem and network effects point to the risk of leveraging market power from adjacent markets. For instance, the association of Cloud Infrastructure Service Providers in Europe (CISPE), filed a complaint to the EC[58] in November 2022 regarding alleged Microsoft practices to leverage their market position in productivity software services into the cloud services.

iii. Switching and interoperability barriers

The market is characterized by extremely low churn due to high barriers to switch. That means it is difficult to move software applications or data from one cloud (ecosystem) to another. Issues can be related to portability of data, interoperability of APIs and pricing structure. Because of the limited interoperability between the providers each provider has its own ecosystem. System Integrators try to build services on multiple clouds. However, at least for the time being and subject to the effects of the incoming implementation of the DA, most multi cloud customers use the different clouds for different purposes and workloads.

iv. Barriers to entry and expansion

The physical infrastructure of cloud data centres requires a substantial investment with important economies of scale associated with the size of data centres, acting as a barrier to entry and expansion for cloud providers. Therefore, *hyperscalers* operate significantly further data centres and in more regions than smaller cloud providers[59], because of the size and global reach of their data centres and larger global customer base. The high initial investments (high CAPEX) are a threshold for other providers to enter the market. Only a very few providers have the deep pockets and self-supply to build a data centre without even before having prospective clients[60].

Investments in research and development (R&D) to develop custom hardware involve high fixed and sunk costs and technical expertise, which may act as an additional barrier to entry and expansion for smaller cloud providers. In this regard, TM Forum concluded[61] in 2022 that Google, Facebook, Amazon and Microsoft spent 70 times more on R&D than four big ECN/S operators (AT&T, BT, Deutsche Telekom and Telefonica). Such difference is explained in the report for the decision made by most operators to outsource their technology development to vendors and systems integrators. The leading ECN vendors (Ericsson, Huawei and Nokia) spend a similar proportion of their total revenues on R&D as big techs although, in absolute terms, they are behind due to the differences in revenues. According to this analysis, while ECN/S operators' R&D investments are mainly driven to reduce costs, Big Tech's R&D

[58] https://cispe.cloud/cispe-files-complaint-against-microsoft-with-european-commission/

[59] For example, according to OFCOM's report, Microsoft Azure operates between 200-350 and OVHcloud operates 33 data centres.

[60] This was confirmed by stakeholders in the interviews with BEREC. Also, the French NCA has calculated that it requires between 500-700 EUR millions to build a data centre. Autorité de la Concurrence Avis 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud ») https://www.autoritedelaconcurrence.fr/fr/avis/portant-sur-le-fonctionnement-concurrentiel-de-linformatique-en-nuage-cloud

[61] Telco to techco: capex and opex implications. 2022. https://inform.tmforum.org/research-and-analysis/reports/telco-to-techco-capex-and-opex-implications

investment is very diverse and covers data centre infrastructure (such as chips, servers, power and cooling); networks (network automation, traffic analysis, subsea-cable technology, streaming platforms) as well as new product areas. This investment in R&D allows them to design and construct their own facilities, network elements and platforms.

5. Interoperability, standards and switching

5.1. Interoperability and standards

As BEREC had already the opportunity to discuss[62], interoperability is "*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*"[63].

Where they pursue objectives other than competition (e.g. data protection), interoperability measures are also designed from the point of view of competitive dynamics and aim to remove obstacles to competition, in particular problems of consumer "lock-in"[64].

Interoperability does not require interoperable systems or components to be uniform, but some common understanding on the exchange of information, e.g. *via* interfaces which can be based on open standards developed, for instance, by standards setting organisations. In order to be interoperable, undertakings providing systems or components set interfaces or implement standards at the edge of their services and products in order to allow the exchange and use of information.

This definition, particularly broad, encompasses a large array of practices:

i. Vertical interoperability or protocol interoperability: the exchange of information between a main system and one or several complements. It would then allow the complementary system to run on the primary system.

ii. Horizontal interoperability or full-protocol interoperability: the capacity to exchange information between several similar systems for the purpose of end-to-end communication. It would for instance allow end-users of competing systems to communicate with each other.

iii. *Data* interoperability: allow the mere exchange of data, not for the purpose of making a system work, nor for the purpose of end-to-end communication. It may

[62] BEREC report on interoperability of Number-Independent Interpersonal Communication Services (NI-ICS), BoR (23) 92, 08.06.2023.
[63] IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, 1990, page 42, see: http://www.mit.jyu.fi/ope/kurssit/TIES462/Materiaalit/IEEE_SoftwareEngGlossary.pdf
[64] OECD, Data portability, interoperability and competition of digital platforms, Background Note, 1 December 2021 https://one.oecd.org/document/DAF/COMP(2021)5/fr/pdf

then concern a lot of different applications. For instance, it may allow users to port their data from one system to another, continuously and in real-time.

As a remedy, interoperability has been used for many years to address competition issues: in several competition law cases (see for instance, Case T-201/04, Microsoft v Commission) and in several *ex ante* regulatory frameworks (see for instance, articles 39 or 61 EECC).

Interoperability is central to the provision of ECN/S as their provision necessarily involves the co-operation of multiple elements or systems. Thus, the telecommunications industry has developed along the years standards and protocols that allow different networks and devices to communicate with each other. This has been facilitated by private associations (e.g. the GSMA) and supported by public bodies[65] since the earliest stages of the telecommunications. Along these years, a common understanding of the mutual benefits of interoperability and cooperation mechanisms with this end have been established.

In the last few years, interoperability gained a renewed interest. Through its different forms, interoperability has been presented by academics and policy makers as a way to address market failures on several digital markets and to ensure the full potential of data-driven innovation by providing opportunities for the exchange and the reuse of data. Interoperability, which is not an end in itself, can be an efficient tool to foster competition, the exchange of data, users' choice, and innovation. It may allow (*i*) addressing lock-in effects related to switching costs and direct network effects, (*ii*) mitigating disadvantages related to economies of scale and scope, by allowing the sharing of data, or (*iii*) preventing leverage effect through self-preferencing practices, by imposing access to platforms on fair, reasonable and non-discriminatory terms. Recently, the Data Governance Act[66] (as well as sector-specific regulations[67]), DA and the DMA have established several provisions to foster interoperability of digital services.

The cloud and edge sector makes no exception in terms of the importance gained by interoperability. Interoperability provisions in the DA will serve the objective of mitigating the technical barriers to switching by facilitating portability from a provider to another. Furthermore, interoperability is also presented as a way to promote a multi-cloud environment and limit the capacity of vertically integrated "*providers to leverage a strong position in part of the services and transfer it to other services*"[68]. Such measures would for instance allow several products and services from different cloud providers to be link and work together. It will promote users'

---

[65] About interoperability regulation in the telecommunications sector see, for instance, CEPT report 107 regulating interoperability https://docdb.cept.org/download/455

[66] Regulation (EU) 2022/868

[67] Proposal for a regulation of the European parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final, explanatory memorandum: "*Sector-specific legislation on data access is in place and/or under preparation to address identified market failures in fields such as the automotive industry, payment service providers, smart metering information, electricity network data, intelligent transport systems, environmental information, spatial information, and the health sector. The current proposal supports the use of data made available under existing rules without altering these rules or creating new sectoral obligations.*"; We can also mention products connected to the Internet of Things since the Data Act will allow for a greater exchange of data in this field.

[68] ACM, "Market study Cloud services", ACM/INT/440323, 05.09.2022, page 61.

choice by mitigating leverage effects: users could choose solutions from different providers either at the same level for different workloads or at different levels of the value chain (*e.g.* IaaS to SaaS).

Standardisation plays an important role for interoperability. It can be induced by *de facto* standards, that is to say standards that are developed unilaterally by a market player. If access to this standard and its implementation is not hindered, and if it shared by a significant part of the market, it can then become a way to make different systems operated by different providers interoperable. This is for instance the case of Kubernetes that was developed by Google and then made available. Alternatively, interoperability may rely on de jure standards, that is to say standards that are elaborated collectively within standards setting organisations (SSO), such ETSI or ISO. Such a process guarantees that the standards are open. Public authorities may play an important role in fostering the development of such solutions. In this regard, the DA, the DMA and the EECC task public authorities to encourage or even mandate drafting standards when needed to implement interoperability remedies.

Another dimension of standardization in the cloud sector is creation of data spaces[69]. The creation of data spaces is sometimes coupled with data infrastructure, as in the case of Gaia-X initiative[70] This European initiative develops digital standards and governance that can be applied on any cloud or edge stack, with the aim to make data and services across different clouds transparent, controllable, portable and interoperable.

An example of interoperability initiatives in the electronic communications cloud world is project Sylva[71], aimed at stabilising an open-source telco cloud software framework. The project was born out of a desire to reduce complexity and to accelerate cloudification of networks within EU's privacy security and energy efficiency requirements. The Linux foundation Europe started this project in 2022 together with two vendors, Ericsson and Nokia, and five carriers, Orange Telefonica, Telecom Italia, Vodafone, and Deutsche Telekom. The Sylva stack will be built on opensource software and has the aim to be interoperable with different clouds and network hardware. Other examples, also led by Linux foundation, are Nephio[72], aimed at NFV and based on Kubernetes, or the Open Gateway project mentioned in chapter 6.3.

According to the interviews carried out by BEREC, some stakeholders perceive that private initiatives by themselves, although proactive and positive, cannot substitute a regulatory intervention to reach a "comprehensive" solution taking into account the technical, economical, strategical factors of the current evolution scenario. The EU is working in diverse initiatives to foster interoperability and standardization. One example is the Smart middleware platform (so

[69] Data spaces refer to the semantic integration of data from different sources and leaving the data stored at the source. The distributed architecture of data spaces allows data redundancies and can be nested and overlapping so that individual participants can be part of multiple data spaces.
[70] https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf
[71] https://sylvaproject.org/
[72] https://nephio.org/

called “Simpl” [73]) to enable cloud-to-edge federations and support major data initiatives funded by the EC, such as common European data spaces. By offering interoperability mechanisms, Simpl will provide generic common services for the establishment, management, and federation of cloud and data spaces. Simpl is to have a minimum viable platform published in 2024.

5.2. Switching

This section further describes existing contractual and business practices that affect switching, by looking into the likely effects of those practices on consumer choice and companies’ ability to compete and, finally, by considering the late normative changes which have been established to facilitate the adoption of multi-cloud and the switching of cloud services providers in the EU.

Currently, the cloud sector is experimenting an important growth and the focus of providers is primarily to convince end-users to migrate their on-premises workloads to the cloud or to gain the business of new digital companies. Several of the agents interviewed by BEREC expressed that, nowadays, considerations about future switching did not feature prominently as a client’s priority when adopting the cloud (switching from on-premise to cloud services) and that instead clients were focused on the cloud safety and functionality. Moreover, several interviewees referred to the prevalence of cloud switching as being relatively small, albeit expected to grow in a small number of years[74]. Most stakeholders agree that switching barriers may become a greater problem in the coming years, as the market becomes more mature, and, thus, welcome the DA measures to facilitate interoperability and switching[75].

5.2.1. Barriers to switching

The decision to change cloud provider or migrate from on-premises to the cloud is rarely simple. Cloud users are diverse, and the switching decision and complexity depend on multiple factors:

i. The complexity and/or specific IT needs of each user vary according to: i) The client’s IT architecture. Switching is more complex when clients use integrated cloud services

[73] https://digital-strategy.ec.europa.eu/en/news/simpl-cloud-edge-federations-and-data-spaces-made-simple-updated-august-2023

[74] Indeed, as established in section 1.2, the take-up of cloud services is small in many European countries and several publications predict large growth rates for cloud services. Unfortunately, the statistics on cloud switching are almost non-existent. According to the Context Consulting Survey (slide 106), in the UK (a leading European market on the take up of cloud) 18% of cloud users had switched PaaS/IaaS provider completely, 35% had taken on additional PaaS/IaaS providers, 35% had considered switching and 23% had never considered switching. In another study, the ACM establishes that users of cloud services seldom change cloud provider (source: section 6.1, ACM (2022) “Market Study on Cloud services” available at https://www.acm.nl/system/files/documents/market-study-def-public.pdf (last visited on July 19, 2023).

[75] BEREC gathered stakeholders’ views and proposals in the Workshop on Switching and Interoperability of Data Processing Services organized in April 2023. A summary report of this event is available in BEREC’s website: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-data-act-workshop-workshop-on-switching-and-interoperability-of-data-processing-services

(IaaS, PaaS and SaaS). Moreover, some providers offer a portfolio of products, in an ecosystem, that may not be feasible to replicate by other providers and ii) the degree of integration of those cloud services with their on-premises IT facilities.

ii. The client's availability of skilled technical expertise to assist and deliver on the migration process and, in particular, the expertise in a determinate cloud/IT environment. The need to retrain staff, especially IT staff, features prominently as a limiting factor of switching. Learning how new cloud services work is dear and, as a consequence of the technical differences among clouds, training is cloud-specific. The French NCA Study[76] describes these training costs and those created by the need to technically integrate services as sunk and a hurdle for switching.

iii. The economic complexity of offers, that may hinder the comparison among different providers (e.g., cloud credits, volume discounts, bundles). Especially, if contractual and pricing conditions are not transparent and if there are difficulties in forecasting future data processing needs by the users so that they are unable to properly align their needs with the pricing schemes of providers (e.g., volume commitments) and are therefore exposed to bill shocks and future lock-in.

iv. The amount of data the client moves from one cloud to another and on the contract signed with the cloud provider, given current pricing practices (e.g., egress fees).

v. Criticality of downtime periods or failure of the switching process.

Therefore, how easy it is to change suppliers is context specific and depends on each customer type[77].

According to the Context Consulting Survey 2023 commissioned to support OFCOM's market study[78], time and cost are the most important challenges to switching. Even if IaaS is the most standardized of all cloud services, ACM (2022) points at lack of or partial data portability as a difficulty in changing IaaS providers, as sometimes data has to be re-formatted before any transfer takes place. Switching SaaS is complex as well, usually even more than IaaS. The Context Consulting Survey identifies app portability as the second most cited challenge by those with switching experience.

[76] Ibid p.24.

[77] This is reflected in the research of Context Consulting (2023) which concluded that among cloud switchers, 7% found switching to a new cloud provider very easy, 40% quite easy, 24% neutral, 23% quite difficult and 6% very difficult.

[78] https://www.ofcom.org.uk/__data/assets/pdf_file/0031/256459/context-consulting-cloud-services-market-research-summary-of-findings.pdf

BEREC's switching experience

BEREC also takes advantage of the usage of cloud services. As a public body, the acquisition of the services is made by tender procedures. Thus, BEREC needs to be prepared to switch cloud provider every time the contract expires. This has been the case in 2023.

In this regard, BEREC (and, in general, the public sector) is different to a private sector agent by the requirements to perform procurement by tenders, on a regular basis. Therefore, BEREC needs to bear in mind the possibility of changing provider in the future when contracting cloud services. For the selection of provider, BEREC considered the risks of vendor lock-in, price, cybersecurity and service resilience, backup solutions and legal considerations such as the requirement of storage within the EU.

BEREC's own experience of its recent cloud switching process, speaks of the need to carefully plan for all the steps involved (the planning stage lasted around 6 months), the necessity to be assisted by the initial cloud provider to ensure a smooth transition as well as additional external support to carry out the migration (with this end, BEREC hired the services of an specialized company), and, finally, of the complexity of the process overall (cost and time -three months were necessary to carry out the switching) and results in considering that BEREC would only envisage changing cloud providers every ten years.

5.2.2. Pricing practices

Part of the success of public cloud services has been attributed to the "pay as you go" pricing structure which enables clients to pay for the use of IT services (GB of storage or per second of computing power) required at every moment. In this way, the user avoids large up-front costs to acquire hardware and software licenses and benefits from the possibility to scale up or down the computing resources.

Providers may charge fees when transporting data in (ingress) and out (egress[79]) of the cloud[80]. The amount of the fees depends on the geographical origin and destination of traffic (whether traffic is in the same region, country or continent) and on the amount of data transported (in case of tiered volume pricing).

Contracts for standardized solutions, aimed at the mass market, have no fixed term and allow for contract termination at any point in so far egress fees are satisfied and no initial commitments have been taken up in the form of cloud credits. These are initial discounts offered to any new client which entail some form of "commitment", whether this is a minimal contract duration or more frequently a promise to achieve a certain level of expenditure (volume discounts).

[79] Egress fees are billed per unit of data transferred out of the cloud, independently of whether this happens because of ordinary course of business or because a cloud contract is terminated.

[80] Also, within the cloud.

Contracts that cater for larger clients and/or for those with specific needs generally entail a larger expenditure and result from an initial client-provider negotiation. In particular these contracts have a fixed term (3 years or more) and their prices are characterized by sizeable conditional rebates and client commitments.

i. Egress fees

Regulators[81] have reported on the important differences on egress fees between providers. Those of the three hyperscalers are substantially higher than those of medium size rivals - by a factor of 5 to 10[82].They have concluded that these fees seem disconnected of the underlying cost of providing transit. For some clients, the expenditure resulting from these egress fees is insurmountable and cannot be compensated by any discounts the incoming supplier may offer, thus constituting a barrier to switching, (especially for clients with large datasets to be moved across clouds) and a risk for competition on merits.

At the same time, in order to entice new business, ingress fees are generally nil and therefore not compensating for the costs of transporting data in the cloud. It should be noted that egress fees need not be the only way by which providers recoup the costs caused by the termination of a contract. For example, these costs could be anticipated and be factored in other service prices, as it happens for the ingress services[83].

ii. Cloud credits, minimal contract commitments and other rebates

The cloud sector is also characterized by upfront discounts that providers offer to gain new clients. Some services are offered temporarily for free (for a few months or a certain number of hours). Other discounts are provided under the client's acceptance of contractual conditions that result in a certain commitment to the suppliers' business (for example, by agreeing to spend a minimal amount and/or by signing a deal for a certain number of years). These conditional rebates, or *cloud credits*, normally increase with the size of the deal and are offered to clients with large and complex requirements. Some regulators explain that in the case of hyperscalers cloud credits can be quite substantive.

---

[81] See Table 2 in ACM report, Figure 18 in French NCA report and figure 5.10 in OFCOM's report.

[82] Their analysis has also shown striking differences between the pricing structure of hyperscalers and other cloud providers (like OVH Cloud and Oracle). Whilst the later set one price per unit transferred out of the cloud with independence of the volume transferred, the hyperscalers use a tiered pricing structure, where the egress fee is highest for transfers between 10 TB and 40 TB and decreases after this. Moreover, the hyperscalers offer free transfers for the first 100 GB.

[83] Moreover, some cloud providers do not use egress fees and instead offer semi-flat tariffs, flat tariffs or even egress services at no cost. Proposals along these lines were suggested by some stakeholders at a recent BEREC workshop on this matter. See, BEREC Summary Report on the Workshop on Switching and Interoperability of Data Processing Services https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-data-act-workshop-workshop-on-switching-and-interoperability-of-data-processing-services

Whilst conditional rebates in the cloud sector have recognized efficiency effects, depending on their size, structure and the commitments entailed, they may erect barriers to switching and multicloud and are difficult to replicate by competitors.

iii. Difficulties in anticipating cloud expenditures

Cloud services are paid per unit of use. This makes it difficult for clients to anticipate their future expenses as they need to predict their demand, which can be problematic in dynamic situations or when market conditions are uncertain or fluctuate[84]. In addition, when a client signs up with a cloud provider, he agrees to a menu of prices of complementary services, some of which may not be perceived as relevant at the point of signature. The difficulty to anticipate expenditures is more acute for first-time "clients", who may even not have the demand metrics required to calculate expenses.

Some authorities have pointed at the consumers' inability to predict cloud expenses[85] and some have explained that in occasions price clarity or transparency is lacking[86]. A few studies have reported on the relevance and frequency of budget overruns[87]. These difficulties could affect switching in two ways: (i) by hindering a client's ability to predict the total volume of egress expenditures to be faced if terminating the contract, and, (ii) by blurring the comparability of the current deal with that of any possible alternative.

Yet, several factors mitigate this problem. First, providers have made efforts to facilitate expenditure predictions. For example, hyperscalers provide consumers with cost calculators with which they can produce forecasts. Second, some existing pricing methods partially[88] overcome the problem of predictability - for example minimal expenditure commitments. Finally, once clients gain expertise in the cloud sector, they will be better at understanding their needs and predicting expenditures.

5.2.3. Effects of barriers to switching

In many markets, consumers and businesses face costs when switching from one service provider to another. These switching costs are expenses or negative effects a user incurs or perceives when switching from one provider to another. Switching costs give providers a certain market power regarding users which use or buy the service on a regular basis.

On the one hand, switching costs incentivise service providers to set low prices for new users to gain market shares. This can lead to intensive ex-ante competition in the initial decision for a specific provider. In cloud markets the above-mentioned low ingress fees for transferring

[84] This is especially relevant for start-ups.
[85] See, for example, ACM (2022) page 27, under "Price".
[86] See, for example, OFCOM (2023) paragraph 5.176.
[87] State of the Cloud report, Flexera, Figure 37 reports an average overrun of 13%. New Cloud Survey | Pepperdata reports that that 33% of the 750 interviewed IT professionals had experienced cloud budget overruns of 20-40%, and 8% even bigger. Available at: New Cloud Survey | Pepperdata, last visited 19 July, 2023.
[88] Nevertheless, predicting what may be the right budget may be problematic.

into the cloud and low upfront costs by pay-as-you-go pricing models can be interpreted as strategic choices by providers to compete for new customers.

On the other hand, switching costs can incentivise providers to set prices high for current locked-in users. Ofcom (2023) finds that more than half of all contract renewals and renegotiations result in a rise of prices. Contract renewals and renegotiations may also involve in agreements of purchase of additional services beyond the originally identified needs in order to keep spend discounts.[89]

Especially with practices of bundling of different (vertically integrated) services and the relevance of complimentary services (e.g. of ISVs on cloud marketplaces) high switching costs may contribute to market concentration through increased economies of scale, scope and indirect network effects. Customers might be less willing to switch away from an established provider, possibly losing investments into the compatibility of all used services. In turn, software developers and complementors focus on compatibility and availability with established cloud providers. These barriers to entry to markets may be additionally higher if the services are complex and tailored to specific needs of customers.

5.2.4. Regulation of switching barriers

The regulation of switching barriers is not new and not specific to cloud services. For example, the EECC provides in Article 106 for transparency requirements when switching internet access services and specifies the process of porting the number when switching number-based interpersonal communication services. Article 107 ensures that bundling of services may not lead to additional contractual obstacles to switching.

In the EU, the policymakers' understanding that competitive cloud markets, fair data access and control are key for economic and societal development led to different measures to promote pro-competitive market initiatives and market rules related to switching of cloud services. The most relevant ones in the context of cloud and edge services are the DA and the DMA.

i. Regulation of switching barriers in the Data Act

The DA has been established to facilitate switching between data processing services and *"encompasses conditions and actions that are necessary for a customer to terminate a contract for a data processing service, to conclude one or more new contracts with different providers of data processing services, to port its exportable data and digital assets, and where applicable, benefit from functional equivalence"*[90]. Accordingly, the DA covers the reduction of contractual, monetary, informational and technical switching barriers.

The DA obliges data processing providers to remove commercial, technical, contractual and organisational obstacles, which inhibit customers from effective switching. With this aim, it defines requirements on the contractual terms between the provider and the customer of data

[89] See Ofcom (2023), paragraph 4.31 and 5.135 and following.
[90] See, recital 84 DA

processing services (e.g. transparency and portability of data) and obligations to provide the customer with relevant procedural and technical information for switching. Providers must allow customers to terminate their contractual agreement of a service within a maximum period of 30 days[91], after a maximum notice period of two months. This Regulation establishes the gradual withdrawal of switching charges up to the 12 of January 2027 when providers of data processing services won't be able to impose switching charges on the consumer, including egress fees.

Nevertheless, some limitations in the DA switching and multicloud obligations are to be considered:

- While IaaS services are subject to comprehensive interoperability ensuring "functional equivalence" after switching, other service types are to be subject to lighter technical requirements regarding switching (e.g. publicly available open interfaces).
- Data processing services that have a majority of features which are custom-built or developed for an individual customer are excluded from the obligations to provide functional equivalence and the withdrawal of switching charges as well as of some of measures to ensure interoperability and standardization to allow switching.
- As mentioned in chapter 2 the definition of data processing services that delimitates the scope of application of the DA might not include cloud and data processing services when they are not scalable or shareable (mainly impacting private networks).

ii. Regulation of switching barriers in the Digital Markets Act

Cloud-computing services are defined as one of the core platform services (CPS) of DMA. While all obligations in the DA are symmetric and address all providers of data processing services independently of size, the DMA entails obligations addressed to designated gatekeepers for these CPS. These obligations are generally defined for all CPS, thus, not all of them are applicable for cloud services[92] and while the designation of the first six gatekeepers includes hyperscalers (e.g. Amazon, Alphabet/Google, Microsoft), such designation regards to other CPS they also provide, and not to their cloud computing services[93].

[91] Where the 30 days deadline is technically unfeasible, it can be extended up to a maximum of 7 months.

[92] Among the obligations in the DMA that could potentially apply to cloud computing services in case that a gatekeeper was designated, Article 5 (8) gatekeeper shall not require business or end users to subscribe to, or register with, any further core platform services (e.g. operating system, web-browser or number-independent interpersonal communication services like video conferencing services). Furthermore Article 6 (6) provides that gatekeeper shall not restrict technically or otherwise the ability of end users to switch between, and subscribe to, different software applications and services that are accessed using the core platform services of the gatekeeper.

[93] See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

6. Cloud and electronic communications interplay

Cloud computing, jointly with hosting and Content Delivery Networks (CDN), are the elements of the internet ecosystem[94] where server computers are run, delivering the content and applications provided by Content and Application Providers (CAPs). Originally, network operators and cloud computing providers were present in different layers of the internet value chain. Nowadays, the relationships between them are increasingly intertwined.

As noted by OFCOM[95], cloud technology is also changing how ECN/S are developed and delivered to customers and is expected to play an increasing role in fixed and mobile telecoms, with partnerships constantly emerging between cloud providers and telecoms providers. About these developments, Professor Martin Cave has underlined[96] that *the cloudification' of networks brings a potential new array of giant firms into the game* and provides two examples of this: i) cloud native operators, such as Rakuten or US Dish (whose infrastructure fully runs on AWS code) and ii) the provision of private 5G networks by cloud providers (mainly, hyperscalers)[97].

Although network virtualization started to be developed over 20 years ago, 5G has been labelled as the first generation of "cloud native network" meaning that for the first time the ECN was designed to work fully integrated with cloud resources. ECN/S operators are transforming their networks towards virtualized and cloud-native architectures. Network virtualization not only allows operators faster deployments at a lower cost, transforming CAPEX into OPEX, efficiencies and more flexibility in the operation or the services but also moving up into adjacent sectors in the value chain and adopt the business model of digital service providers by the provision of NaaS. Furthermore, the capillarity of traditional ECN is an important asset for the deployment of edge computing infrastructure. All in all, cloud technologies present some opportunities for ECN providers enabling the monetisation of their network, leveraging their extended network coverage and privileged access to users and to create value beyond pure connectivity.

On the other hand, cloud providers, in particular hyperscalers, are striving to move their services closer to the user, deploying their own ECN (e.g., submarine cables), leveraging their wide IT services portfolio and their leading presence in the internet ecosystem, including sometimes entering into the traditional telecommunications domain. These investments were in some cases first motivated by the need to enhance communication between their data centres or with some customers to cope with the exponential cloud computing traffic growth,

[94] See BoR (22) 167, BEREC Report on the Internet Ecosystem, 12-12-2022, see: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem
[95] OFCOM (2023) "Cloud services market study: interim report" available at https://www.ofcom.org.uk/__data/assets/pdf_file/0029/256457/cloud-services-market-study-interim-report.pdf
[96] Martin Cave, The achievement of digitalisation in the EU and its reliance on gigabit connectivity, Telecommunications Policy, 2023, https://doi.org/10.1016/j.telpol.2023.102592.
[97] BEREC has also reflected on this matters in the BEREC Report on the 5G Ecosystem BoR (22) 144 https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-5g-ecosystem

and, thus, aimed to self-provision ("make instead of buy"). With the time, some cloud providers have started offering ECN/S to 3rd parties making use of this infrastructure[98].

The extent to which hyperscalers will penetrate further in the value chain is still unclear. On the one hand, cloud providers are far to reach the capillarity of access network providers and according to the feedback by stakeholders, they are not interested in competing with ECN/S in the EU. In this regard, the distributed nature of edge services will require that the computing resources are brought closer to the end-user or device, making operators' capillarity a key asset to be exploited. On the other hand, Amazon[99] and Google[100] already provide mass market mobile services in the United States (US)[101] and, as further explained in the 5G Ecosystem Report and also pointed out by stakeholders, hyperscalers can be well placed to provide, independently of traditional operators, vertical users with value added fully integrated services based on 5G.

For the time being, cloud providers and network operators search for collaboration. The drivers for these partnerships for cloud providers are i) achieving full connectivity (complementing sometimes their own resources), connecting business premises to cloud services and offering edge services by exploiting the extended footprint of geographically distributed data centre locations of network operators and ii) leverage the close relationship of network operators with a large number of users[102].

ECN/S also seek to cooperate with cloud providers both i) to be able to offer advanced services to the users and ii) for the functioning of their own networks. In the first case, they reach partnerships with cloud providers to resell cloud services and offer bundled IT and ECS services or to provide cloud-based network services (NaaS). In the second, operators are further collaborating with cloud providers in the transformation and migration of network workloads and other essential functions to the cloud. Moreover, cooperation could be beneficial in order to improve network performances or avoid congestion related to cloud services traffic.

In both cases, partnerships allow cloud providers and ECN/S benefit from the know-how and experience in their respective areas. Furthermore, by moving ECN now to the cloud there is a chance to set standards and gain intellectual property as part of the first mover advantages.

---

[98] For further information about these developments, see Draft BEREC Report on the general authorization and related frameworks for international submarine connectivity BoR (23) 214 https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-the-general-authorization-and-related-frameworks-for-international-submarine-connectivity

[99] https://www.amazon.com/b?ie=UTF8&node=20429280011

[100] https://fi.google.com/about

[101] In the case of Amazon, connectivity is bundled with Prime, benefiting from ecosystem effects that can be attractive for the uses.

[102] For example, AWS has partnered with Vodafone in Europe to deploy Multi-access Edge Computing (MEC) services in the data centres at the RAN edge of the mobile network operator. https://www.vodafone.co.uk/newscentre/press-release/partnership-aws-wavelength-launch-first-multi-access-edge-computing-services-in-europe/

Therefore, for the time being, the complementary nature between cloud and connectivity is generally fostering the cooperation between ECN/S and cloud providers, driven by the mutual supply of services and commercial partnerships, whereas an increasing competition is already observed in specific business areas. These different cooperation/competition dynamics are better understood by exploring the main areas where cloud and edge services interplay with ECN/S.

6.1. Connectivity to cloud and edge

Linked to the location of data centres from where cloud services are delivered, the first type of interaction between cloud and telco domain regards connectivity. Although hyperscalers also deploy their own connectivity infrastructure, generally cloud providers require the supply of network connectivity by ECN/S operators (i) to enable customers to access their data and services in the cloud, and (ii) to interconnect the geographically distributed data centres of the cloud provider.

i. Connectivity between the data centre and the end-user

The connectivity between the data centre and the end-user is either provided over public internet or by means of dedicated communication depending on the specific needs of the service. Many enterprises reach the cloud providers' data centres over the public internet through the broadband connection provided by their Internet Service Provider (ISP), just as consumers do. However, large businesses and global companies with high-capacity requirements and critical applications in the cloud often prefer not to rely on a single connection to the public internet. In these cases, network operators supply dedicated and/or managed network connections between the business customer premises and the cloud provider location, thus increasing redundancy and reliability.

Furthermore, the main cloud providers also offer the possibility to directly connect to their clouds in different locations or through network partners[103].

ii. Connectivity among the data centres

The decentralized and broad network featuring cloud services imply the deployment of a widespread number of data centres that require reliable and secure connectivity among them.

For both types of connectivity (with the users and among the data centres), cloud providers can choose between making resort of a third-party, such as ECN/S providers, or deploying their own.

In this regard, hyperscalers are investing in the deployment of their own dedicated network infrastructures, including submarine cables, fibre or satellite networks to interconnect their data centres worldwide. There are several drivers for these investments:

[103] Some examples: AWS Direct Connect, Microsoft Azure ExpressRoute, Google Cloud Interconnect.

i. cope with their increasing data traffic growth;
ii. increased control of the provision of the services;
iii. better guarantee the performance and resilience of the customers' applications, services, and data in the cloud;
iv. facilitate a highly secure, reliable and available private network.

6.2. ECN migration to the cloud

ECN are evolving from vertically integrated service specific networks to virtual environments in which network and service functions are performed by software instead of dedicated physical resources. This evolution has been facilitated by the application in the ECN domain of virtualisation methods already used in IT, such as SDN (Software Defined Networking)[104] and NFV (Network Function Virtualisation)[105].

Virtualisation allows network functions and resources to be delivered through software running on VMs executed on general-purpose hardware devices. This solution allows operators reducing costs, run software services from multiple vendors, facilitate the programmability of electronic communications networks and promote the efficient use of computing resources.

These Virtualized Network functions (VNF) are already available in many networks and increasingly hosted in cloud infrastructures. VNFs are evolving towards Cloud-native Network Functions (CNF) which are designed as microservices and implemented to run inside containers[106], that can be easily moved between virtual environments.

The transformation of ECN to cloud based networks would be mainly driven by the enhanced network scalability, reduced network complexity and increased operational efficiency reached with cloud migration[107]. Such advantages include:

i. Facilitate the deployment of functions that would be more easily scaled, updated and orchestrated,
ii. Reducing CAPEX, as network applications can be replicated on demand,
iii. Lowering OPEX, since software updates could be performed without interrupting user services and failure recovery would be more agile,
iv. Reduce dependency on suppliers, as the cloud-native architecture enables the porting of applications across different providers.
v. Enhance network capacity management to serve new regions or customers by scaling cloud resources. Additionally, auto-scaling (allowing idle network assets to be dynamically shut off and brought online as required), if well-orchestrated, can enable

[104] SDN enables the functions of a network to be controlled by software. It has therefore removed the previous close integration between network hardware and network functions.
[105] NFV is a type of virtualisation in Electronic Communications Networks (ECNs). It provides virtualisation of network functions meaning they can be shared in the physical network by a number of services. Therefore, network functions are no longer physically located.
[106] The containerisation allows bundling the application along with all the necessary files for its execution.
[107] According to a survey led by CapGeminy Research Institute. https://www.capgemini.com/insights/research-library/cloudification-of-networks

more efficient use of networking resources, leading to lower energy use and thereby reducing the telco network's overall carbon footprint.

While network operators are at different stages on their transition of ECN towards cloud native architectures, most of them are progressively deploying CNF alongside VNF, in particular for 5G networks. The 5G technology architecture itself allows for cloud-native deployment of the core, called 5G SA core – making it the default choice for greenfield deployments. The broad range of forecasts available agree on the assumption that migration of network functions, operations and business support to cloud offer tangible benefits and is expected to grow[108].

This progressive adoption of cloud technology affects all network domains: Core Network, RAN, backhaul and transport network, network operation and orchestration (OSS) and business support (BSS).

However, the cloudification of ECN is also challenging. Networks are restricted by geography and are configured to provide service in particular areas. This means that, in the case of certain network domains, scalability benefits of cloud in ECN may be less pronounced than for public clouds, because networks require a margin of local unused resources to support unexpected peak demands. Functions not tied to a geographical area, such as BSS, allow systems to be scaled efficiently and, thus, are expected to benefit further from cloudification. Further, according to the External Study, given the global scale of mobile networks and vendors, cloud-based business support would have more scale benefits for mobile networks than for fixed.

As observed from interviews with stakeholders and the OFCOM report, most operators are still reluctant to move network workloads to public cloud and prefer the migration to a private cloud, suggesting hybrid cloud as a possible cloud architecture approach. Some drawbacks to using public cloud for electronic communications specific workloads mentioned by stakeholders include the lack of control, resiliency and security reasons or uncertainty about the costs of public cloud adoption.

6.2.1. Core Network

In the core, cloud is used for applications that require significant processing power and large storage space. It's also the part of the network where most critical functionalities and sensitive data reside. Therefore, operators seem hesitant to incorporate public cloud providers into this area[109].

This situation is expected to change in the coming years, as some agreements are already being reached with hyperscalers to incorporate 5G core workloads into the public cloud. This would allow operators to leverage the scalability advantages of public clouds for handling

[108] The External Report provides quantitative market data from several sources. For example, one of them estimates that 31% of global network capacity is being serviced by cloud today, and this is expected to increase to 46% in the next 3 to 5 years.

[109] According to the Capgemini report (Ibid p 41), 82% of surveyed companies prefer using internal private clouds for their core network.

unexpected increases in demand and benefitting from the specialized tools for data processing and analysis provided by these cloud providers.

Dish in the United States was the first operator to build its 5G core network in the public cloud of AWS[110]. Traditional network operators and suppliers in Europe have also begun collaborating with major public cloud providers. Recent examples include O2 Telefónica in Germany, which partnered with Ericsson and Google Cloud for a joint deployment of the 5G core network[111], and Swisscom, which is conducting a pilot project with Ericsson and AWS to explore hybrid cloud operation scenarios for Ericsson's 5G core network[112]. This includes offloading workloads to the public AWS cloud during traffic peaks or when performing maintenance tasks on Swisscom's private cloud.

6.2.2. RAN edge

In the course of network disaggregation and the cloudification, many ECN/S providers plan to leverage Cloud RAN[113] (C-RAN) architectures to centralize baseband processing functions and ultimately undertake their virtualization.

5G systems, in particular, support different functional splits in the radio access protocol stack that enable flexible placement of RAN functions, their hoteling and cloudification. This enables intelligent scaling of computing resources as demand on capacity fluctuates and improves operational efficiency at cell sites. By launching dynamically virtualized instances on demand, C-RAN also enables operators to address different use cases by locating compute and storage resources at different locations within the network according to use case requirements/needs. These edge locations can also host ECN/S providers' own applications or ECN/S providers' partners applications, for example, by supporting latency-sensitive applications through cloud edge solutions that are collocated with the serving cell site, thus realizing the paradigm of Multi-Access Edge Computing (MEC).

The virtualization and the cloudification of the RAN (Cloud RAN and, virtual RAN vRAN) has also put forward an increasing trend for opening interfaces between the different components of the disaggregated RAN. Open RAN is an example of this initiative aiming at fulfilling such trend, while several challenges (technical, operational etc.) have to be overcome before the related benefits would materialize as reported by the BEREC Workshop on Open RAN[114].

Figure 7 illustrates the trend towards the RAN "cloudification", featuring the functional splitting, remoting/hoteling and cloudification.

---

[110] https://aws.amazon.com/blogs/industries/telco-meets-aws-cloud-deploying-dishs-5g-network-in-aws-cloud/

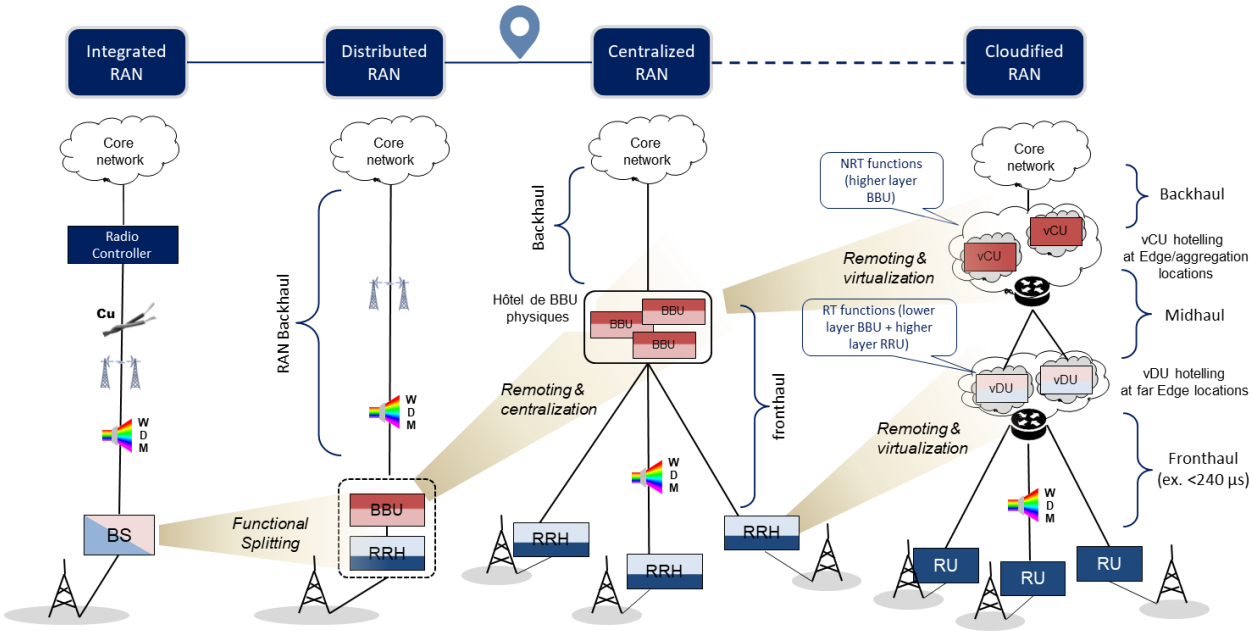
[111] https://www.telefonica.de/news/press-releases-telefonica-germany/2022/12/network-of-the-future-for-new-5g-solutions-o2-telefonica-lifts-5g-core-network-into-the-cloud-to-unlock-new-opportunities.html

[112] https://www.ericsson.com/en/news/2023/3/swisscom-ericsson-and-aws-collaborate-on-5g-core-for-hybrid-cloud

[113] Cloud RAN architecture implements parts of the radio access network as virtualized network functions in a data centre.

[114] https://www.berec.europa.eu/en/events/berec-events-2022/berec-workshop-on-open-ran

Figure 7 The evolution of the RAN architecture towards RAN "cloudification"



BS: Base Station, BBU: Base Band Unit, RRU: Radio Remote Heads (a.k.a Radio Remote Units)
RU: Radio Unit, vDU: virtualized Distributed Unit, vCU: virtualized Centralized Unit
NRT: Non Real Time, RT: Real Time

Source: ARCEP

The deployment of a larger edge footprint involves both investment and maintenance costs. For this reason, mobile operators and infrastructure providers are seeking for collaborations for the deployment of computing solutions at the network edge. So, operators are gradually expanding their points of presence. Infrastructure providers, especially those with neutral host solutions, can potentially play an essential role in increasing the number of locations and computing resources that can be shared among multiple tenants.

In addition, the operators are also exploring mutually beneficial commercial agreements with other stakeholders, especially cloud service providers, for the development of edge services. These providers, particularly hyperscalers, have significant economies of scale in providing cloud infrastructure and services. They are also looking to expand their business into small-scale and affordable cloud service offerings near the customer to offer their range of data processing applications in a low-latency, highly reliable, and privacy-compliant environment. Consequently, the convergence of both objectives is leading to collaboration agreements between network operators and cloud providers to extend the deployment of edge computing services.

Private networks are one of the primary use cases for deploying edge computing resources, where there are examples of this collaboration, as public cloud providers have released edge

solutions on enterprise premises or at the telco network. In this sense, many MNOs have started to launch MEC[115] in collaboration with cloud providers. AWS Outpost is used by Verizon to offer private 5G networks to businesses at their locations[116], and AWS Wavelength computing and storage services are located within the 5G mobile operators' data centres at the network edge, such as in Vodafone UK[117].

Microsoft and Google are also establishing similar partnerships with operators for the deployment of edge computing solutions. These are non-exclusive agreements in which network operators provide their central offices as hosting locations. For example, Telefonica has partnered with Microsoft on Azure Private Edge Zone to integrate their 5G private industrial connectivity and edge computing capabilities on customer premises[118], and also with Google Cloud's Mobile Edge Computing platform for the joint development of a 5G solutions portfolio[119].

6.2.3. Backhaul and transport network

The virtualization and cloudification of network functions pose several challenges on the underlaying connectivity infrastructure, particularly for the backhaul, fronthaul and midhaul part of the network[120].

The traditional concept of mobile backhaul refers to the transport network that connects 4G Base-band Units (BBU) or 5G Centralized Units (CU) with the mobile core network. Mobile fronthaul refers to the transport network that connects the Remote Radio Heads (RRH) to centralized BBU as used in 4G centralized RAN architectures or where 5G Radio Units (RU) are connected to remote distributed units (DU). Additionally, midhaul refers to the link between the DU and CU in the 5G network.

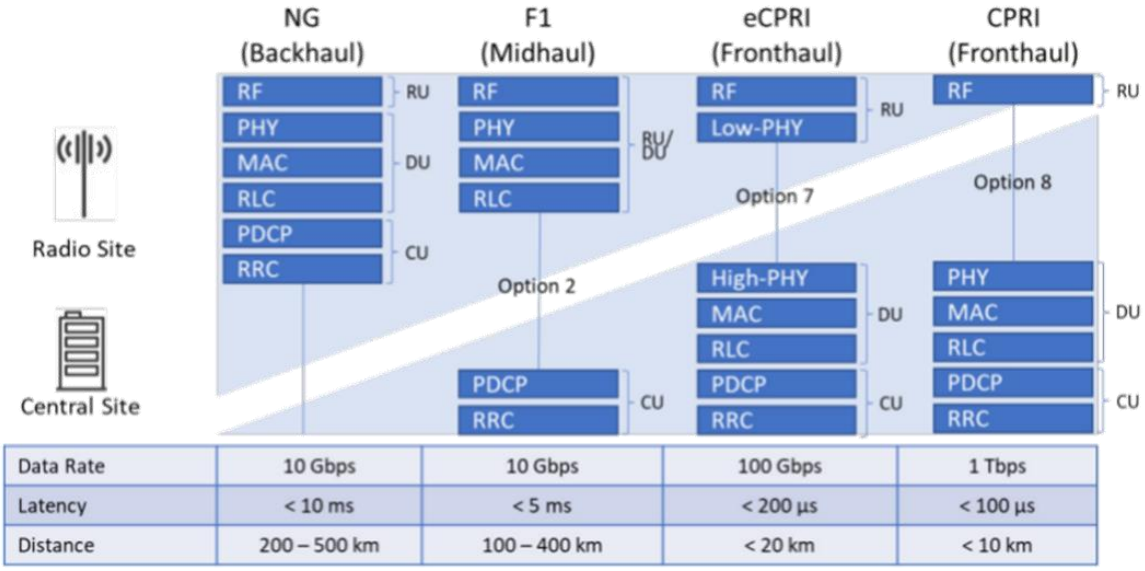
Moving process-intensive functions to an aggregation site requires the stricter transport bandwidth and latency requirements associated with backhaul/fronthaul/midhaul networks. 4G backhaul/fronthaul networks of today, typically implemented using semi proprietary protocols such as Common Public Radio Interface (CPRI) over dark fibre or microwave systems, are costly to build and maintain and may not cope with the trend towards a higher capillarization of the radio access network and increasing QoS requirements of the transport links in terms of capacity, latency/jitter, timing (synchronization) and fixed-mobile convergence. Figure 8

[115] MEC services offer application developers and content providers cloud-computing capabilities and IT service environment at the edge of the mobile network. https://www.etsi.org/technologies/multi-access-edge-computing
[116] https://www.verizon.com/about/news/verizon-private-mobile-edge-computing-enterprise-aws-outposts
[117] https://www.vodafone.co.uk/newscentre/press-release/partnership-aws-wavelength-launch-first-multi-access-edge-computing-services-in-europe/
[118] https://www.telefonica.com/en/communication-room/press-room/telefonica-tech-partners-with-microsoft-to-provide-the-industrial-sector-with-private-5g-connectivity-and-on-premises-edge-computing/
[119] https://www.telefonica.com/en/communication-room/press-room/google-cloud-and-telefonica-partner-to-accelerate-digital-transformation-for-spanish-businesses/
[120] F. Rayal "RAN Virtualization: Unleashing opportunities for market disruption", Xona Partners, June 2016.

shows how data rate and latency requirements vary according to the selected option for functional splitting in the RAN protocol stack.

In addition, to get the most out of 5G advanced features (such as network slicing), the xhaul[121] transport network infrastructure should also be ready to support automated, smooth and zero touch connection reconfiguration for network/IT load placement between the edge cloud locations in one hand and between edge cloud and central cloud in the other hand.

Figure 8 Transport requirements for some selected 5G RAN functional splits.



Source: 5G America Whitepaper "Innovations in 5G Backhaul Technologies IAB, HFC & Fiber" June 2020

Meanwhile, MEC can also relieve backhaul requirements. While incurring a cost to implement core functions at the edge, MEC can also provide opportunities to optimize backhaul demand via caching and/or local breakout[122]. For example, the "User Plane Function (UPF) at the Edge" solution in 5G allows selected core network functions, such as the user plane gateway function, to be deported at edge locations for performance or traffic isolation considerations.

Caching reduces the load over mobile backhaul and enhances the customer experience by allowing the storage and process frequently accessed contents in the edge network. Customers can access the contents at a lower latency and xhaul demand is reduced as there is no need to reach further to the external network to retrieve the contents.

[121] Xhaul is a generic term standing for anyhaul and referring to backhaul, fronthaul and midhaul transport networks, interconnecting radios, base stations and Edge Clouds.

[122] Local breakout entails the provision of an internet access point located as close to the user as possible enabling to route the traffic directly to the internet,

Local breakout also enables the mobile xhaul transport infrastructure to be optimized as the contents/application data do not need to travel through the core network and then to the internet. The caveat with local breakout is that the xhaul network connecting the edge to the internet needs to be in place and with the required quality and therefore it may not optimize cost in certain scenarios.

6.2.4. Network operation and orchestration (OSS) and business support (BSS)

ECN operators are migrating the back-office and IT functions, such as billing, service management and customer relationship management towards the public cloud environment.

Instead of maintaining complex on-premises infrastructure, operators can deploy BSS[123] and OSS[124] systems in the cloud, with easier accessibility, rapid deployment, and the ability to scale resources based on demand to offer a better customized customer experience and benefit from cost savings.

The administrative processes which support BSS and OSS applications are being rapidly virtualised and automated in data centres. However, although both BSS and OSS are being moved to the cloud, it seems that BSS workload migration to the cloud is further ahead, as OSS allocation to the cloud is driven by network function virtualisation (NFV) in the network[125].

6.3. Provision of cloud-based network services

5G mobile networks evolve towards a service-based cloud architecture (SBA), where network functionalities and capabilities can be deployed on demand and made accessible to third parties through APIs, similar to the provision of other cloud services.

SBA allows operators to explore new methods of monetizing their network infrastructure and expand their revenues, by enabling the creation of a service development platform for developers and solution integrators, specialized in the creation of digital services for consumers and businesses in different vertical sectors. This model of network service provisioning is generally referred to as "Network as a Service" (NaaS), as it allows access to virtualized network services and infrastructure on-demand through a pay-as-you-go model.

The development of these APIs is being undertaken in collaboration with various organizations, both standardization bodies (such as ETSI and 3GPP) and industry associations (such as GSMA and the Linux Foundation). Many of these efforts are focused on

[123] BSS are the IT systems supporting the business and customer operations. They are usually considered to include revenue management and customer-care systems.
[124] OSS systems support the service and network operations. They usually include service fulfilment and delivery platforms, network management systems (NMS), and more recently the network orchestration systems.
[125] Omdia's 2021 OSS/BSS Evolution survey found that communications service providers are more likely to embrace cloud-native technologies for systems in the BSS domain.

edge computing (MEC, EDGEAPP, Telco Edge Cloud). However, the goal of operators and other members of the industrial association GSMA is to create a common platform by means of the Open Gateway initiative.

The initiative Open Gateway[126], led by GSMA, is a framework of common network APIs designed to provide universal access to operators' networks. The Open Gateway aims to provide a technology layer easily accessible to application developers and cloud providers, allowing them to integrate network capabilities into their platforms in an easy and accessible manner.

These standardized APIs are defined within CAMARA, an open-source project led by the Linux Foundation in collaboration with GSMA, according to the requirements established by the Operator Platform Group to achieve network interoperability among operators. Thus, developers can configure their services for all users, independently of their operator, with the same API.

Operators are collaborating with service aggregator companies where the largest communities of digital service developers are located, such as *hyperscalers*, and Communication Platform as a Service (CPaaS) providers like Vonage[127]. This collaboration aims to showcase and expose the capabilities of Open Gateway and begin creating services and applications based on the already available APIs.

6.4. Bundled and integrated ECS and IT services with cloud

As indicated in the BEREC external Study on Communication Services for Businesses[128], the practice of bundling telecom and IT services is well established.

According to this study, in 2022, business customers declare having subscribed to a bundle including ECSs along with collaborative solutions and/or cloud storage for 40-50%, regardless of the company size and 30-40% of other IT services within an ECS bundle. The demand-side survey shows that most organizations are planning to keep the share of bundle subscription unchanged for the future: 68% among large organizations and 62% among SME. The main reason to buy these bundled products, in addition to cost considerations and simplification of contractual procedures by one-stop-shop, is the better integration of the services. 59% of large organisations and 50% SME reported to choose bundles for this reason. The organisations

[126] Open Gateway was presented at the 2023 Mobile World Congress in Barcelona and was launched with the support of 21 global mobile operators. https://www.gsma.com/futurenetworks/gsma-open-gateway/

[127] Ericsson acquired the cloud communications provider Vonage in 2022

[128] Based on a survey among 1.000 business users from France, Germany, Italy, Poland and Spain (200 in each country) https://www.berec.europa.eu/en/document-categories/berec/others/external-study-on-communication-services-for-businesses-in-europe-status-quo-and-future-trends

with multiple sites are also more likely to be motivated by this potential benefit (53%, versus 46% for single site organisations).

According to operators, the most frequent IT services bundled with ECS are mainly security (firewalling, anti-DDoS), cloud storage or server hosting, Unified Communications and Collaboration (UCC) [129] and Software Defined Wide Area Network (SD-WAN). From the demand side, 40-50% of business customers declare having subscribed to a bundle including ECS along with collaborative solutions (e.g., Teams) and/or cloud storage, regardless of the company size, and 30-40% of them within an ECS bundle with other IT services (dedicated server hosting, IaaS, SaaS and security services).

All interviewed operators agree on the fact that traditional ECS revenues will decrease while IT services have the greatest potential for development in the coming years. In addition, the provision of UCC services that combine various communication channels such as video conferencing, messaging, or call centre services blurs the lines between the traditional provision of electronic communication services by operators and that of equivalent cloud service providers[130].

ECN/S operators have diversified their traditionally connectivity-focused services for businesses incorporating adjacent IT services, such as cloud, cybersecurity, and data analytics, as a way to increase their revenues. By leveraging their data centre infrastructure, network operators usually propose hybrid and multi-cloud services to enterprises, varying from dedicated private cloud or traditional IT hosting, until shared environments where companies can migrate their IT workloads to the operator's own cloud or to the public cloud of hyperscalers through collaboration agreements[131].

Thus, ECS and IT services providers appear to be in an increasing competition, in particular for the growing Business to Business (B2B) market opportunities. However, based on the informal interviews BEREC has kept with several stakeholders, most of them agree that partnerships will still be very essential in the short/medium term, as no one covers the whole value chain.

On the one hand, hyperscalers are focused on scalability and technologies, such as data analytics and AI/ML, and are less prone to go up to the last mile. Although entering into the ECS domain for business customers, especially in private networks, customer relationship is a challenge and hyperscalers may prefer to collaborate with operators to reach all business customers and build tailored solutions to their different needs, as telcos have local

[129] UCC can include email, voicemail, calendars, scheduling tools, video conferencing, instant messaging, desktop sharing and VoIP. Additionally, it may include presence tracking, which is the ability to tell whether a contact is busy or free, and unified messaging, which is the ability to retrieve all messages from a central location.
[130] Such as Amazon Connect, Google Voice or Microsoft Teams.
[131] For example, Telefonica provides their own public IaaS cloud service based on VMWare and offers managed services and expert staff in the public clouds of hyperscalers: AWS, Google Cloud, Microsoft Azure, Oracle Cloud Infrasructure and Huawei Cloud Services. https://cybersecuritycloud.telefonicatech.com/en/solutions/cloud

infrastructures with trusted commercial relationship, built upon the connectivity services they already provide.

On the other hand, telecom operators have their own public cloud infrastructure and services, but they lack the economies of scale of cloud providers and cannot offer the huge number of services that hyperscalers include in their portfolio[132].

Therefore, operators are establishing collaborative agreements with these big cloud providers, becoming resellers and technical experts of their public cloud services, adding specialized data protection and security services combined with their own data centre hosting, in order to differentiate themselves from the hyperscalers.

Data sovereignty requirements are having an impact on the market. Thus, operators usually propose their own storage and hosting services to business customers, highlighting this is a differentiating factor for organisations that have concerns about the location and access to their confidential data and applications. They offer professional services to build hybrid or multicloud solutions adapted to customers' demand. Likewise, it is expected this collaborative trend will keep growing, given the possibility of bringing cloud capabilities closer to the users, at the edge of the network, to offer real-time or near-real-time processing, and enable local treatment and analysis of IoT based massive data[133].

However, ECN/S operators are concerned about their ability to compete on an equal footing due to the ease of access to capital of some of these companies and fear they might be downgraded to a support service. As examples of these concerns, some stakeholders draw attention to the hyperscalers provision of services that could compete with ECN/S providers in B2B private networks, such as the deployment of 5G private networks as a managed service (e.g. AWS Private 5G in the US), or the networking trend towards SD-WAN technology[134]. The external study mentions that some IT services do come with their own integrated or bundled cloud solution[135]. These tying and bundling practices are considered an issue that needs to be properly addressed, and it has been already highlighted in other cloud reports[136].

[132] Operators in BEREC external study mentioned that some IT services do come with an integrated cloud solution. Thus, Microsoft 365 was by default bundled with Azure (both owned by Microsoft) and Salesforce linked with AWS hosting (global partnership between both companies).
[133] As example, MNOs have started to launch Multi-access Edge Computing services (MEC) in collaboration with cloud providers.
[134] For example, AWS includes a Cloud WAN service. Cloud WANs depend on SD-WAN (software-defined WAN) technology, which overlays the physical WAN infrastructure with an intelligent software layer. It provides simpler management for the entire Wide Area Network.
[135] Microsoft 365 was by default bundled with Azure (both owned by Microsoft) and Salesforce linked with AWS hosting (global partnership between both companies)
[136] Such as ACM Market Study on Cloud Services or the Pr. Frédédéric Jenny report for CISPE, October 2021 https://cispe.cloud/studies/fairsoftware

7. Network cloudification regulatory considerations

7.1. Network cloudification in the EU Regulatory framework

One of the overarching principles of the EU Regulatory Framework is technology neutrality. This principle entails that regulation shall be agnostic of the underlying technology used to provide the services so that providers can be free to select the use of the technology that they deem most appropriate and this regulation can remain sufficiently stable despite of the technical and technological changes that may take place in the highly dynamic digital markets.

Along these lines, recital 14 EECC reminds the need to adjust the definitions "*to ensure that they are in line with the principle of technology neutrality and to keep pace with technological development, including new forms of network management such as through software emulation or software-defined networks".* Therefore, the EECC mandates to consider SDN or NFV for ECN/S definitions and, consequently, the scope of regulation.

As part of the preparatory work for the last regulatory framework review that eventually led to the EECC, the EC requested BEREC to issue an Opinion on Potential Regulatory Implications of Software-Defined Networking and Network Functions Virtualisation[137]. An input paper was delivered in 2016.

In this analysis, BEREC mentioned the uncertainties related to the fact that SDN and NFV were at their early days of development. With this caveat in mind, some considerations regarding the regulatory impacts of SDN and NFV were considered in relation to: i) access to passive network infrastructure; ii) Fixed network access; iii) Mobile virtual networks and sharing of network elements; iv) Network costs calculation; v) changes in the value chains.

As a general conclusion, BEREC called for the new regulatory framework *"to be flexible enough to cope with the dynamic development of SDN and NFV and the uncertainty of the outcome of this development (…) and ensure that NRAs will be able to respond to this dynamic development of SDN and NFV appropriately".* As seen above, this call was taken on board by the EU co-legislators.

BEREC notices that, although SDN and NFV are still to be broadly implemented by all ECN operators, some uncertainties have been clarified since 2016: greenfield operators are deploying cloud-native networks and brownfield operators are progressing in the same direction. Further clarity regarding changes in the value chain, roles and interactions among the different players has also been gained in the last 7 years.

[137] https://www.berec.europa.eu/en/document-categories/berec/others/input-paper-on-potential-regulatory-implications-of-software-defined-networking-and-network-functions-virtualisation

Moreover, in February 2023, the EC carried out an exploratory consultation on the future of the electronic communications sector and its infrastructure. The main takeways of this consultation were published in October 2023[138]: the EC stressed the feedback received regarding the significant impact on the electronic communications sector of network virtualization, edge cloud, AI and open networks and concludes that network transformation towards new software-based, highly programmable, cloud-native networks "*will have a significant impact on business and regulatory models, skills, infrastructures, security of vendors and of course investments".*

Against the backdrop of the results of this public consultation, Commissioner Breton announced an upcoming proposal for a Digital Networks Act (DNA)[139] making a call to "*create the conditions for the sector to fully embrace the technology shift towards cloud-based software-defined models. Telecoms networks are becoming "network-as-a-service", where connectivity and computing capacity converge thanks to edge technologies and physical switches become application programming interfaces (API)".*

The DNA has eventually taken shape by means of a proposal for a White Paper - *How to master Europe's digital infrastructure needs?[140],* published on 21 February 2024 for public consultation until 30 June 2024. The White paper proposal, among many other issues, makes a call to reflect on *technology convergence between telecoms and cloud, which are nonetheless subject to different regulatory frameworks[141].*

Considering the evolution of cloud-based networks, the new information available and the announced legislative initiatives, those initial regulatory implications of network cloudification could be reviewed and developed. These thoughts may also feed the analysis of the EECC review due by 21 December 2025.

7.2. Potential Regulatory Implications

7.2.1. Insights provided by the External Study

On 12 December 2023, BEREC published an external study on the trends and policy/regulatory challenges of cloudification, virtualisation and softwarisation in telecommunications[142] (the External Study), aiming at informing BEREC's work.

The Study develops on the issues and trends associated with cloudification, virtualisation and *softwarisation* in the provision of ECN/S. It encompasses: i) the description of current technical state of the art related to network virtualisation, the identification of the key players in the value chain and the use cases, and ii) a more analytical analysis regarding the identification of

[138] Available in: https://digital-strategy.ec.europa.eu/en/library/results-exploratory-consultation-future-electronic-communications-sector-and-its-infrastructure
[139] See: https://www.linkedin.com/pulse/digital-networks-act-redefine-dna-our-telecoms-thierry-breton/
[140] https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs
[141] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_941
[142] Ibid. P. 11

potential regulatory and competition issues and challenges and of the expected future trends, including possible new business models that may be enabled by virtualization.

The potential regulatory challenges gathered in this Study include: i) the impact of the migration to cloud-based networks may have on the vendors ecosystem and competition; ii) the potential of hyperscalers of impacting competition in adjacent markets, including ECN/S markets; iii) the potential disadvantages for smaller ECN/S operators to compete on equal footing at a global scale; iv) the role of NRAs in favouring investment (including network upgrades); v) the role of NRAs to prevent digital exclusion regarding the affordability of enhanced services and devices for end-users; vi) emerging challenges regarding security of networks and data and vii) the environmental impact of this technology evolution.

7.2.2. BEREC's regulatory considerations

Based in the abovementioned previous work and inputs as well as the additional research and information gathered for the elaboration of this report, BEREC identifies that the following trends and issues may have an impact in the sector and, thus, require to be considered by regulators:

i. Scope of sectoral regulation

As BEREC has noted before[143], one of the main updates of the Regulatory framework in the EECC was the review of the definition of ECSs.

The EECC takes into consideration the functionality provided by the services independently of the underlying technology used. Such general approach for the definition of the services is applied as well on cloud-based networks, in line with the abovementioned recital 14 EECC. Therefore, in general terms, the substitution of physical elements by software elements would not impact the definitions and, thus, the scope of application of the EECC.

However, the practical implementation of this general approach may not be always straightforward. As described in chapter 6.4, ECN/S, IT and cloud/edge computing services are increasingly intertwined. Also, due to the current and expected evolution of new digital services, the boundary between ECN/S and the cloud services provided (most of them, currently out of the scope of regulation) becomes more and more blurred. As services gain complexity, a case-by-case assessment will be required.

[143] See, for instance, the BEREC Report on the interplay between the EECC and the EC's proposal for a Digital Markets Act concerning number-independent interpersonal communication services: https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-interplay-between-the-eecc-and-the-ecs-proposal-for-a-digital-markets-act-concerning-number-independent-interpersonal-communication-services

Such cloud and ECN/S convergence may also lead to overlapping of the rules and jurisdictions by different competent authorities in charge of their implementation leading to complexities in understanding the legal environment that apply to both cloud services and ECN/S provision.

Some authors have also reflected on these convergent trends. For instance, A. Manzalini and N. Crespi [144] indicated that *"'this evolution towards SDI will definitely blur, on one side the border between the Telecommunications networks and the Cloud Computing, and, on the other side, the distinction between the Telecommunications networks and the future "terminals" connected to them* (…) *because of this evolution, several economists, as well as technologists, have started to wonder if the usual representation of relationships among a myriad of players in a certain industrial area can still be modelled on the bases of value chains. There is a growing consensus that value chains modelling shall be complemented by a broader view considering business ecosystems. Current regulation should evolve to support this digital economy, making it sustainable."*

In brief, whilst the ECN/S definition has served its purpose in the context of traditional services but also with Internet-based services, it is worth analysing if it is sufficiently future proof and clear enough to guarantee legal certainty in the context of services convergence.

Such analysis should consider the general frame provided by BEREC in its Action Plan 2030[145]. Namely, the Action Plan acknowledges the changes taking place in the sector including virtualisation and cloudification and the replacement in some cases of traditional ECS by new digital services and platforms. BEREC also points out that it has to adapt its approach to regulation to include (new) digital services and platforms and their providers in its portfolio to reflect the changing remit and the broader scope of activities of the NRAs. Consequently, one of the BEREC actions in the Plan is to be also a trusted and independent expert body on internet-related and digital matters.

ii. Competition implications on the ECN/S markets

Network cloudification requires new expertise and resources beyond the traditional ECN provision. While some operators have started this journey together with the hyperscalers (e.g., AT&T/Azure[146] or Dish/AWS[147]) others, such as Rakuten, have decided to build its own solutions and, subsequently, are commercializing their solutions to other ECN providers (e.g., 1&1[148] in Germany). Some have pointed to the potential issues stemming from increasing

[144] A. Manzalini and N. Crespi, "SDN and NFV for Network Cloud Computing: A Universal Operating System for SD Infrastructures," 2015 IEEE Fourth Symposium on Network Cloud Computing and Applications (NCCA), Munich, Germany, 2015, pp. 1-6, doi: 10.1109/NCCA.2015.11.

[145] https://www.berec.europa.eu/en/document-categories/berec/others/berec-action-plan-for-2030

[146] See: https://news.microsoft.com/2021/06/30/att-to-run-its-mobility-network-on-microsofts-azure-for-operators-cloud-delivering-cost-efficient-5g-services-at-scale/#:~:text=DALLAS%20and%20REDMOND%2C%20Wash.,managed%20using%20Microsoft%20Azure%20technologies

[147] https://aws.amazon.com/blogs/industries/telco-meets-aws-cloud-deploying-dishs-5g-network-in-aws-cloud/

[148] See e.g. https://global.rakuten.com/corp/news/press/2023/1208_01.html

interdependences in the provision of ECN/S[149] such as the introduction of big cloud providers into the electronic communications world. As further develop under point v, there is a risk that big tech leverage their privileged market position in digital services such as cloud into adjacent markets, including electronic communications. However, migration is still at an early stage, technical solutions and standardization are still being developed and experiences may significantly differ.

NRAs/BEREC should remain vigilant on the evolution of cloud markets and, in particular, of the types of dependencies and relationships cloud providers have with ECN/S operators, the access to relevant inputs or reaching necessary agreements for the provision of the services on equal footing in particular, for smaller providers. Competition problems in cloud markets could result in damages to competition or impact users' choice in electronic communications markets. In that case, it should be assessed whether existing legal instruments (e.g. competition law) are sufficient to address these issues or if new rules need to be put in place.

Moreover, the virtualization/cloudification of network functions may create asymmetries among network operators as not all are equally equipped to face the inherent challenges or move to the cloud. Indeed, they may be less able to bargain good deals with cloud providers and may not be the best placed to take build or buy decisions. Therefore, NRAs/BEREC also need to stay vigilant in this respect.

iii. Competition implications on cloud markets

ECN operators own and control the last mile network infrastructure close to end users (featuring great capillarity) and might be in favourable position to provide certain edge computing applications enabled by network cloudification.

Cloud services (provided over the internet) depend on the access networks of ECN operators. These might have the incentive and ability to limit how access to the network is delivered (e.g., by restricting access to APIs, see point vi below). They might be able to leverage their control of the access network into network-based cloud services, resulting in reduced competition and less favourable outcomes for consumers and businesses.

NRAs may follow these developments paying particular attention towards any potential negative effect on the users that might arise from the coordination between ECN/S providers regarding the services provided across this "last mile" infrastructure.

iv. Competition implications of partnerships between ECN/S and cloud providers

Many operators are partnering with big cloud providers to offer customized offers that combine both ECS and cloud services, whereby operators often play the role of managed service provider, acting as technical experts on the public cloud services of the hyperscalers and

[149] E.g. Will the cloud business eat the 5G telecoms industry? https://www.economist.com/business/will-the-cloud-business-eat-the-5g-telecoms-industry/21806999

adding specialized services to cope with business users' requirements such as data protection or security.

Furthermore, ECN/S and cloud service providers are collaborating to explore new revenue streams linked to the digitization of multiple vertical sectors, in particular with the development of 5G networks. This involves combining the enhanced capabilities of these communication networks in terms of increased bandwidth, low latency, and support for multiple IoT devices, with the computing and AI/ML data analysis techniques enabled at the edge of the network. Consequently, the convergence of both objectives is fostering collaborative agreements between ECN operators and cloud providers to expand the deployment of edge computing services.

Although these partnerships are positive for the development of innovative services for customers, BEREC recommends a careful monitoring of these agreements and their effects in downstream markets. ECN/S operators and cloud providers already offering services to businesses have a privileged position compared to other market players. Hence, the combined provision of connectivity and cloud services in specific cases could help in reinforcing their respective market positions and potentially create barriers to entry of new players.

In this regard, operators' relation with business customers can be crucial in directing solutions towards the products and services of specific cloud providers, such as hyperscalers, with whom they have exclusive agreements. This would further strengthen the ecosystem of hyperscalers and network effects and, ultimately, their market position and potential leverage.

Similarly, although hyperscalers generally seek collaboration with multiple connectivity providers, exclusive agreements for the location in the network of edge computing and access to AI capabilities can, in turn, strengthen the market presence of the selected network operator. This can be crucial for the business market and the development of (5G) use cases, in particular for private networks.

These mutual agreements between network operators and cloud providers do not inherently pose a threat to competition and are beneficial for both parties. However, it is important to monitor that they do not imply an implicit collusion, especially concerning access conditions to cloud-based services that may limit customer choice, innovation and the interoperability with other services from alternative cloud providers.

v. Other competition issues related to ecosystem effects

As explained under chapter 4, the cloud market features ecosystems and network effects. In the same vein, BEREC has described the interrelation among the different elements and players of the Internet in the 'Report on the Internet Ecosystem'[150]. Among the conclusions of this report, BEREC underlines that Big Tech companies (including hyperscalers) are present across practically all the elements, or they can enjoy a significant presence in a relevant part of the elements in the internet ecosystem and can often leverage their position among different

[150] https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem

services and products. In addition, and addressing more concretely cloud services, the report points to the concentration of commercial CDN and cloud markets and the significant investments required to have the necessary geographical coverage and capillarity. Moreover, BEREC indicated that the infrastructure of cloud computing services relies on large investments, due to the existence of very significant economies of scale in this market where large companies can leverage their power on other parts of the Internet ecosystem.

In the 'Report on the ex-ante regulation of digital gatekeepers'[151] (issued in the context of the elaboration of the DMA), BEREC called for the consideration of platform ecosystems for the design of regulatory measures in the context of digital markets. BEREC pointed out that being part of an ecosystem reinforces the platform's gatekeeping role while allows it to leverage its power onto additional services, or to have privileged/exclusive access to key inputs/assets raising further barriers to entry or expansion to other operators/providers.

The risk of leveraging market power in the digital ecosystem could impact many different adjacent markets. In the context of this report and, in particular, regarding the interdependencies between ECN/S and cloud providers, it is worth setting a particular focus on AI services.

As mentioned in chapter 2, there are relevant synergies among AI, IoT, 5G and cloud/edge services: AI systems support the automation of network functions for cloud-based networks. In turn, some AI systems would require of the capabilities provided by 5G and edge computing[152]. Thus, network modernization is not only enabled by cloudification but also by implementing AI systems.

Against this framework, BEREC notes that on 8 November 2023, the 'G7 Competition Authorities and Policymakers' Summit Digital Competition Communiqué'[153] indicated that "*Significant computational resources such as cloud computing services and largescale computing power also are critical. An inability to access these key inputs may inhibit competition to develop AI and AI applications, reducing innovation and harming consumers*." Similar concerns around leveraging market power in the cloud sector into the AI market have been voiced by EU stakeholders[154]. Should these concerns materialize, ECN/S dependencies on *hyperscalers* could be reinforced as, in such potential scenario, some network developments would require access to AI enablers. Furthermore, similar leveraging risks may appear to IoT services in view of the mentioned interdependencies.

---

[151] https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-ex-ante-regulation-of-digital-gatekeepers

[152] BEREC further develops on this matter in the Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-impact-of-artificial-intelligence-ai-solutions-in-the-telecommunications-sector-on-regulation

[153] https://www.cas.go.jp/jp/houdou/pdf/betten1-1.pdf

[154] https://www.euractiv.com/section/artificial-intelligence/news/are-eu-regulators-ready-for-concentration-in-the-ai-market

While digital services are complex and require an in-depth and, sometimes, even a case-by-case, assessment, analysing digital competition trends (e.g. AI systems, IoT, cloud/edge services, 5/6G, etc.) as isolated elements misses the broad perspective necessary to understand ecosystem effects and, thus, identify all competition implications, essential inputs, bottlenecks in the provision of the services or barriers to entry for the provision of the services.

vi. APIs openness and API exposure

The disaggregation of the value chain together with multiplicity of stakeholders brought by ECN/S cloudification highlight the key role of APIs. These APIs constitute the “glue” used to orchestrate the interactions between the actors: between the telco-cloud[155] and its customers; between the telco-cloud and its upstream suppliers/partners (cloudified network functions providers, virtualized infrastructure or connectivity providers).

Beyond the first issue related to technical interoperability between API, encouraging the ecosystem and the industry to promote the use of Open APIs[156], other issues related to the exposure of APIs (i.e. how to expose? to whom? under what conditions and according to what modalities?) may have a competition/economic character calling for the attention of the regulator who will have to consider APIs as an object or as a lever of regulation on some kind of “Gate-keeping” or unfairness that may occur regarding market access/service provisioning.

Cloud provider or vendor lock-in because of lack of API openness

Consistent APIs based on open standards allow communication across multi-vendor environments and effectively future-proof the network. Otherwise, the lack of API openness makes cloudified network functions not discoverable and accessible to third-party CNF suppliers, thus restricting the ability of a ECN/S operator/provider to mix and match solutions as desired. This would result in a situation of vendor lock-in where an operator would be forced to select the same supplier as a default choice and not get the best solution. Such a situation of vendor lock-in may occur in two cases:

- a case (illustrated as case 1.a Figure 9) where a CNF from ECN/S provider “A” unable to communicate with CNF from a partner ECN/S provider “B” – lack of openness of APIs on East and Westbound Interface (E/WBI)[157];

---

[155] Although there is no standard definition for Telco-cloud, it refers to a target vision featuring a paradigm where a telecom operator embraces fully the cloud; it describes an evolution of the classical (current) model of telcos into a platform-like cloudified telecom network providers. According to VMWare, "*Telco cloud is a next-generation network architecture that combines software-defined networking, network functions virtualization, and cloud native technology into a distributed computing network.*"

[156] Open API is paradigm for describing APIs in a standardized format that can be read by a machine enabling to indicate to the API user what requests exist and what responses to expect, in an agnostic manner to the API programming language. Although this refers to a specific definition of Open API (API based on open standard), Open API may also refer to other definitions such as API backed by open data (data freely available to use and republish without restrictions).

[157] APIs are categorized as Northbound, Southbound, Eastbound and Westbound based on the direction of communication. API communicating from SDN controller to a higher layer are labelled as Northbound (NBI), to a

- a case (illustrated as case 1.b Figure 9) where an operator is unable to mix and match between two CNF supplied by two different suppliers because they are tightly coupled with the virtualized infrastructure – lack of openness of APIs on the Southbound Interface (SBI).

A similar situation of lock-in may occur because the CNF is tightly coupled with the cloud environment of a given cloud provider/hyperscaler and not being able to be ported (either fully or partially[158]) within the cloud environment of another cloud provider/hyperscaler; this is illustrated through case 1.c Figure 9 and refers to cloud provider/hyperscaler lock-in.

Potential issues related to API exposure

Potential issues related to API exposure may occur in different hypothetical situations[159] :

- Access of ECN/S provider "A" via the SBI interface to the virtualized infrastructure resources of its supplier, which is an entity belonging to ECN/S provider "B" (for instance its cloud arm) and a competitor on the same downstream market (illustrated as case 2 Figure 9);

- Risk of discriminatory or unfair behaviour from ECN/S provider when implementing the NaaS model by providing a set of Northbound Interface (NBI) APIs to a user client X and restricting the access (technically or commercially) to these NBI APIs to another user client Y. The user client may be a B2B customer such as a vertical or an application/service provider (illustrated in case 3 Figure 9);

- Network capabilities exposure (through the NaaS model), and the need to provision API consumers (enterprises, developers etc.) with a consistent multi-Communication service provider API framework, would highlight the role of CPaaS providers (illustrated in case 4 Figure 9).

  CPaaS act as an exposure gateway, transforming network APIs into service APIs. CPaaS may be a Content Application Provider/a hyperscaler, an API aggregator or an ECN/S provider. In the API value chain, developers/enterprises (User "Z") buys services via service APIs from CPaaS providers, who pay ECN/S providers for consuming network functions through NBI APIs (network APIs), ECN/S providers buy network functions and their exposure capabilities (Network NBI APIs) from suppliers to enable advanced B2B and B2C use cases.

  If the platform provider holds a dominant position in the market and is related to a given network function supplier, the latter may go beyond the standardized APIs by

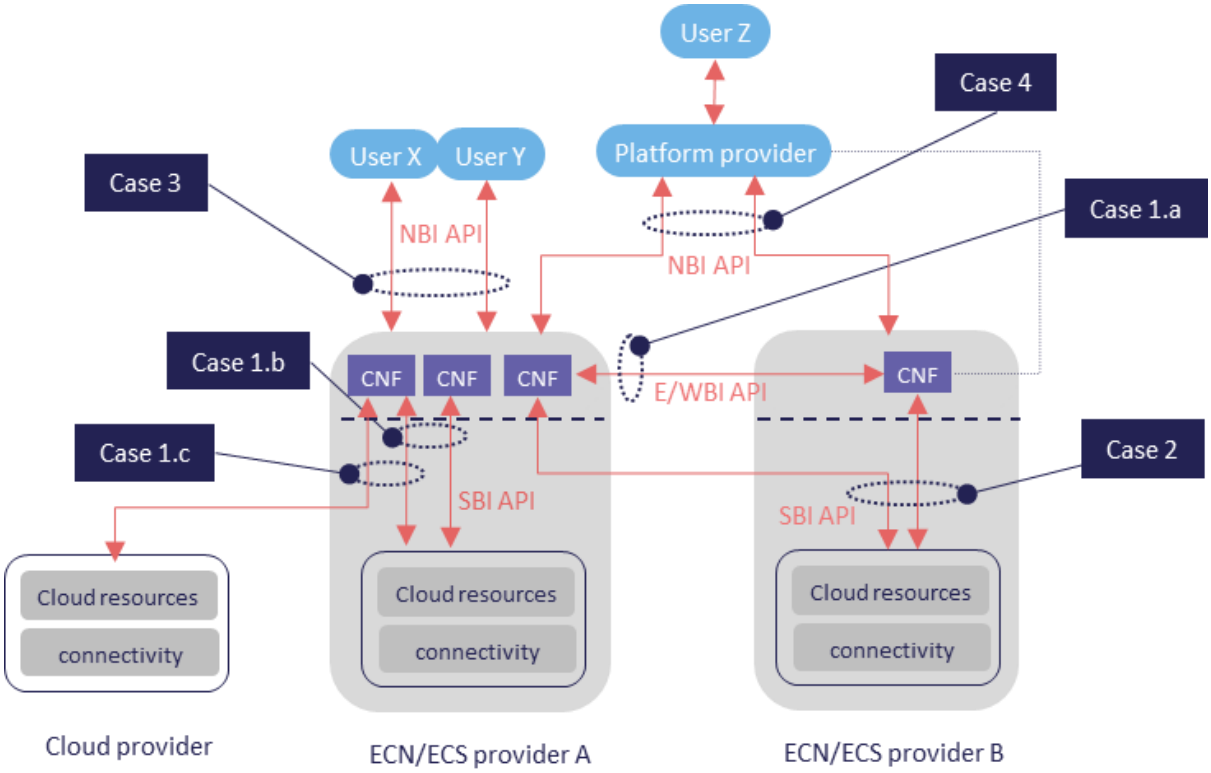
lower layer, Southbound (SBI) and East/West bound (E/WBI) refer to the communication between different servers.

[158] Partial porting may refer to a situation where the CNF is effectively being executed within another cloud environment but at a detriment of performance/expected functionalities.

[159] Because of the emergent nature of this topic, for the time being, the described situations are hypothetical and refer to theoretical cases.

proposing a set of specific and non-open APIs and entices its market adoption by leveraging the position of its platform provider arm. ECN/S provider may end-up in a situation of a closed ecosystem lock-in.

Figure 9 Illustration of the potential regulatory risks associated to API openness and API exposure.



Source: ARCEP

Net neutrality, security and Data privacy considerations

API exposure, as any other technology enabler (slicing, edge computing etc.), would not be considered against net neutrality *per se*, instead this needs to be investigated on a case by case basis[160]; this encompasses the exposure of some NBI APIs dealing with traffic influence, traffic management or Internet access quality of service differentiation, etc.

[160] Further insights regarding net neutrality rules and technological evolution are found in the BEREC Opinion for the evaluation of the application of Regulation (EU) 2015-2120 BoR (22) 163 https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-2015-2120. This evaluation, published in December 2022, concludes that the previous 2018 Opinion on the application of the Regulation is still valid regarding emerging technologies https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-guidelines. Namely, BEREC's conclusions in this regard are as follows: "*BEREC considers that the Regulation leaves considerable room for the implementation of 5G technologies, such as network slicing, 5QI and Mobile Edge Computing. To date, BEREC has no knowledge of any concrete example given by stakeholders where the implementation of 5G technology would be impeded*

Open API solutions and API exposure may also pose challenges in terms of ensuring security across open interfaces in a multi-vendor environment, security of the system when exposing its capabilities and the conformance with privacy requirements (e.g. restricting the API exposure to a specific geographical area to ensure compliance with the applicable data privacy rules such as GPDR legislation) according to the different privacy threat vectors (data privacy, location privacy, identity privacy etc.).

vii. Fostering investment in cloud-based networks

The idea of "network softwarization" emerged in the early 2010s, promising a profound and positive transformation of ECNs towards more open, de-layered and reconfigurable models sustained on the scalability and flexibility procured by the cloudification and virtualization of network functions[161]. However, despite the good omens, network softwarisation is taking more time than initially expected and is being pursued unequally by (ECN) operators. Whilst most have transferred business support activities (BSS) to the cloud (even to the public cloud), the cloudification/virtualization of network functions has been limited to certain operators, networks (i.e. 5G), network activities (i.e. functions related to the control and monitoring of the mobile core control plane and orchestration) and quite generally been undertaken on private clouds.

The benefits of moving network intelligence to a virtualized environment have been detailed in Chapter 6: improvements in operational agility and network flexibility, cost reductions and the origination of a novel model for the development of new services, based on open-access collaboration with software developers (NaaS). Since a key objective of regulation is to facilitate connectivity and access to services for all citizens[162], of special relevance to NRAs duties is the idea that cloud-based networks can facilitate more agile network deployments and operation, as well as their potential for lower prices for services.

Yet, investments are costly, need a clear economic case and are more easily developed in environments with controlled or limited technical and economic risks. The path to network virtualization and cloudification is a substantive leap forward for operators and entails important challenges:

---

by the Regulation. As with all other technologies, the specific use of 5G technologies must be assessed on a case-by-case basis under the Regulation. BEREC welcomes stakeholders to engage in a dialogue with NRAs if stakeholders experience uncertainty whether a specific use of a 5G technology complies with the Regulation."

[161] Epitomizing this, in their contribution to the IEEE 2015 conference, Manzalini and Crespi, concluded that as a consequence of softwarization: "*Service Providers and Virtual Operators fully embracing this innovation wave may see dramatic costs reductions (e.g., estimation of 40%-50% CAPEX savings), improved efficiency in the overall Operations (e.g., estimation of 25%-35% OPEX savings only by automating processes), reduced time-to-market, greater flexibility and adaptability to new emerging service paradigm*s".

[162] Article 3 of the EECC includes the objective to "promote connectivity and access to, and take-up, of very high-capacity networks, including fixed, mobile and wireless networks, by all citizens and businesses of the Union".

i. First, technically it is an important change in network architecture and not an easy transition as it requires innovation and the upskilling of operators' expertise as well as a thoughtful consideration of what should be done and why. From its conversations with different agents, BEREC has learnt that:

- given the current status-quo, the skills required to develop network virtualization are cloud-specific and operators are in a shortage of qualified staff to accomplish (and manage) the innovations[163];
- cloud-solutions are not technically feasible for all network functions and there needs to be a "case by case" analysis of whether it makes sense to take steps in such direction[164]. Considerations about the traffic that is created by workloads and their bandwidth and latency requirements play a decisive role in the choice to virtualize network functions.

ii. Second, some risks accompany the transition to virtualized/cloudified networks. In particular:

- maintaining strong security of data and network reliability while allowing smooth data flows is critical. Even more if the transition is to a cloud owned and managed by a third party to which operators need to relinquish control and responsibility. This is why operators are opting for private clouds over which they keep some control, despite those being less scalable than public ones;
- insufficient interoperability and standardization between cloud-based network solutions create operator lock-in with cloud vendors and hinder the adoption of efficient investments and preferred alternatives. In this sense, a common blueprint for deploying ECS on the cloud that all operators could make use of would be ideal, yet standards take time to appear and may not be sufficiently inclusive, ensuring a level playing field for all;
- economic uncertainties about the degree to which operators may monetize appropriate revenues from the new services enabled by cloud-based networks, as well as more primary uncertainties on their level of demand. Also, for public clouds difficulties in anticipating the costs of operations.

iii. Third, it implies a change in operators' wholesale markets whereas they are transiting from buying network equipment from specialized vendors (to be owned and be managed by operators) to hiring computing and data space resources from cloud providers to be

[163] One of the most advanced operators in network cloudification is AT & T who has established a joint venture with Microsoft Azzure to cloudify some network functions of the mobile core. With the joint venture, the knowledge of network and cloud experts can be combined to develop the solutions needed.

[164] For example, some network functions, like radio management functions DSPs, require a very tight latency and are very well-optimized in the existing status-quo so, with the current state of technology, it makes no technical or economic sense to virtualize those. According to a commentator: "there is no need to reinvent the wheel".

managed by operators. Whether as a result from this, wholesale markets will become more (or less) competitive is very unclear. Both the equipment market and the cloud market are very concentrated, but operators may be cautious about lock-in and on increasingly relying on cloud providers as those compete directly with ECN/S providers for business clients. Moreover, as explained in Chapter 5.2.4, the measures to facilitate interoperability and switching in the DA, may not be fully applicable to ECN/S providers who base their business on a customized product or third-party private cloud, as those are not necessarily under the scope of the regulation or of some of the provisions that have been conceived for mass market products.

In its 'First report on the State of the Digital Decade'[165], the EC has estimated that €148bn funds are needed to reach the Digital Decade targets for Gigabit connectivity and 5G and that a further €29bn-€79bn to ensure connectivity of transport paths. These investments which will sustain improvements in network coverage will co-exist with the needs to invest in network innovation[166].

Like in other sectors, electronic communications operators invest in projects with good expected returns and compete for capital in the global market. More profitable projects outbid less profitable ones. Therefore, even with all the risks described, the opportunities brought about by network softwarisation may imply a shift in operators' investment focus towards cloudification and virtualization, possibly crowding out some of the private investment on extending network coverage. Even if this is not the case, network virtualization/cloudification will exert additional pressure on operator's financing.

Given the objectives attributed by the EECC to NRAs and BEREC[167], they must monitor the technology landscape to assess whether any upcoming developments create risks to connectivity, competition and the internal market and promote efficient investment and innovation in new and enhanced infrastructure while ensuring that competition in the market and the principle of non-discrimination is preserved. BEREC has identified some of the risks that accompany the transition to virtualized/cloudified networks and is developing its thinking on how NRAs/BEREC could assist to "*remove remaining obstacles to, and facilitating convergent conditions for, investment in, and the provision of, electronic communications networks*".

For example, this report and the Study identify that the electronic communications sector would clearly benefit from standardisation efforts to enable complex and interoperable new

[165] 2023 Report on the state of the Digital Decade available at https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade, page 12.

[166] According to ETNO, *Open RAN, Network Function Virtualization, and Software-defined Networks are expected to also have a significant impact in terms of capital expenditure, each falling within the €10 billion to €100 billion range by 2030.* https://etno.eu/news/all-news/786:eu-telecoms-council-etno-calls-to-support-the-european-connectivity-ecosystem.html

[167] Article 3 of the EECC attributes BEREC and NRAs objectives to promote of network connectivity, network take-up and competition in the provision of ECNs and ECS. Also, to contribute to develop the internal market by "removing remaining obstacles to, and facilitating convergent conditions for, investment in, and the provision of, electronic communications networks, electronic communications services, associated facilities and associated services".

systems. Clearly, regulators should promote and remain active in work by technical standards making bodies in order to contribute to the rapid development of efficient and inclusive solutions so that risks to efficient investment and lock-in are safeguard.

viii. Fostering connectivity investment to enable edge computing.

The ambitious goal set by the EU to establish 10,000 climate-neutral and highly secure edge nodes by 2030 will certainly have an impact in the investment dedicated to improving connectivity to enable edge computing and the enhancement of network capillarity.

However, the development of such infrastructure faces some hurdles including the higher complexity associated with deploying and maintaining such massive infrastructure in terms of increased number of devices, regulatory uncertainties and difficult to predict market needs and demand. Moreover, as mentioned in Chapter 6, it's not clear the extent to which hyperscalers will penetrate in the traditional network operator's domain. From the interviews carried out with stakeholders on the scope of this report, a lack of interest from hyperscalers to compete on the ECN/S European market has been identified. ECN operators have an existing, widespread infrastructure that allows them to offer services closer to the end-user, which is critical in edge computing for reducing latency and improving quality of service. This unique advantage positions these operators favourably in the edge computing value chain, potentially enabling them to play a key role in its development and widespread adoption.

Also, it's important to bear in mind the growing significance of "tower infrastructure" companies, commonly referred to as towercos[168], which traditionally have been instrumental in leasing space on towers for mobile network operators. However, their role is evolving in the context of edge computing and they can be a key player in fostering investment for the development of infrastructure to hold edge computing equipment due to its privileged location, close to the end-users and the fact they own the passive infrastructure that can accommodate edge computing devices for specific sector solutions.

The location of edge nodes, much like mobile networks' antennas in the traditional electronic communications market, is one of the key factors that will shape the investment in edge computing. The effectiveness of edge computing largely depends on the proximity of these nodes to the end-users, as it directly influences latency, bandwidth, and overall quality of service. This similarity raises several considerations:

- The placement of edge nodes is key for ensuring efficient data processing and transfer. Nodes need to be located close to users to minimize latency, which is especially important for applications requiring real-time data processing, like IoT devices, autonomous vehicles, and certain types of AI applications.

[168] With regard to the role that towercos play in the EU telecommunications development, see BEREC's External study on the evolution of the competition dynamics of tower and access infrastructure companies not directly providing retail services BoR (23) 206: https://www.berec.europa.eu/en/document-categories/berec/reports/external-study-on-the-evolution-of-the-competition-dynamics-of-tower-and-access-infrastructure-companies-not-directly-providing-retail-services

- In some regions, especially rural or underserved areas, the deployment of edge nodes might be limited, leading to (or maintaining) a digital divide. Ensuring equitable access to edge computing resources could become a concern.
- Public-private partnerships might be necessary, particularly in regions where the commercial incentive for private companies to invest in edge infrastructure is limited.

Given the potential for disparities in access to edge computing resources, regulatory bodies and industry stakeholders might consider measures to promote access. These could include policies to ensure fair access to edge infrastructure, mandates for infrastructure sharing among different service providers, or initiatives to support the deployment of edge nodes in underserved areas. Governments could play a role in subsidizing or incentivizing the deployment of edge nodes in strategic locations to ensure broader coverage.

Having said that, whilst the towercos have a strong position in terms of passive infrastructure ownership and location, the hyperscalers make their case in terms of market understanding, due to the fact that they can identify and offer new services to users in different areas where the user demand is not yet fully understood and they are able to capture the added value of the investments made which increases the chances of improving the RoI.

ix. Interplay amongst the different EU legislations impacting cloud and ECN/S

The EU's digital strategy, commenced in 2020, aims to shape its future digital transformation. Central to this strategy is the EU data strategy, which focuses on enabling the data economy through policies that empower businesses and the public sector to harness data for decision-making. It establishes pillars like empowering individuals and SMEs, creating a cross-sectoral governance framework for data, developing common European data spaces, and investing in data infrastructure and interoperability.

Since then, the EU regulatory landscape, particularly through the DMA, DSA, and DA (and in the future, AIA), has developed a new framework governing (among others) cloud computing services, reflecting the complexity and multifaceted nature of the digital economy.

The DMA targets some large digital platforms, which are designated as gatekeepers, to ensure contestable and fair markets. However, its application to cloud services is not foreseen at this moment, as for the time being, no provider has been designated as gatekeeper for these services. Also, the DA's role in cloud computing is introduced to foster equitable data access and a competitive data market. It brings forth new legal obligations for cloud service providers, especially in terms operational requirements for service switching and interoperability. The DSA, on the other hand, aims to prevent and fight illegal and harmful online content provided by the users of intermediary services, including cloud services.

The interplay between these Acts and other EU digital legislations like EECC, NIS 2, GDPR, Free Flow of Data Regulation, Open Data Directive, AIA and others (see, ANNEX I), is crucial in understanding their collective impact on the digital ecosystem. Moreover, the relationship between the DA and DMA is complex due to overlapping goals, such as fairness and market

contestability, and some of the obligations (to be enforced by different bodies). Similarly, issues of provider switching and interoperability among EECC, GDPR, DMA, and DA require careful consideration to ensure their effective application and legal certainty and avoid creating unnecessary red tape for users and providers.

One concrete example is that, as mentioned under chapter 5, both the DA and the EECC regulate the switching of providers (for data processing services and ECS respectively) including, in the case of the EECC, bundled products. Where a bundled product includes an ECN/S service, the EECC provisions shall apply to all elements of the bundle (thus, including any cloud services included in the bundle). While the EECC aims generally to consumers, these switching provisions may also apply to SME. In those cases, the enforcement of both legislations would have to be aligned.

Cybersecurity considerations, the NIS 2 Directive and the ENISA security certification scheme[169] are pivotal in enhancing data and infrastructure security. They mandate essential entities, including medium and large cloud service providers, to comply with harmonized security and risk management obligations. The evolving cybersecurity certification frameworks like EUCS also play a significant role in shaping the cloud computing market, particularly regarding data sovereignty and security standards.

Legislation in the digital field needs to be aptly tailored to support the growth and efficiency of cloud computing, which is vital for the advancement of the digital economy. These EU's regulatory measures, while aiming to create a fair and innovative digital market, are to be carefully applied to cloud computing services. This necessitates a harmonised approach that addresses not only market contestability and data protection but also the technological specificities and operational dynamics of cloud services.

x. Digital regulatory enforcement

The increasing EU legislation on digital matters[170] should be coupled with an effective implementation of these rules, with different but closely interrelated scope, by means of the consistent application of the different regulatory provisions in a coordinated way, both at national and EU level as well as across the heterogeneity of the competent bodies. The institutional setup should contribute to a coherent and efficient legislative enforcement avoiding unnecessary red tape for the stakeholders.

Along these lines, BEREC has previously warned about the risk of excessive fragmentation of the regulatory tasks among different authorities in the context of its 'High-level Opinion on the DA proposal'[171]. Such fragmentation could undermine both the effective implementation of the rules, due to the difficulties to apply consistently the different provisions of the DA, and also

[169] https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme

[170] As reflected in ANNEX I, in the last 2 years, a number of EU acts impacting the sector have been passed and others are to be approved soon. Among those: DMA (2022), Data Act (2023), Data Governance Act (2022), AI Act (poss.2024), DSA (2022).

[171] https://www.berec.europa.eu/system/files/2022-07/BoR%20%2822%29%20118_BEREC%20H-L%20Opinion%20on%20the%20ECs%20proposal%20for%20a%20Data%20Act_0.pdf

hinder coordination at international level due to the heterogeneity of the national bodies. The same rational is also applicable from the broader perspective of the digital markets regulation due to the tight interlinks existing among the services and their development in ecosystems as well as among the EU legislations.

BEREC understands that cooperation with competent authorities of other Member States is key to achieve the internal EU market and, based on its long experience, recommends that this cooperation is structured on a permanent basis by means of a forum gathering all national independent competent authorities. BEREC emphasizes in particular the need for coordination between (i) different authorities enforcing the same laws across member states (ii) different authorities enforcing different laws addressing the same digital services and providers.

Finally, BEREC underlines the importance of independent bodies to shape stable and predictable regulatory environments, independent of short-term political cycles, industry as well as other stakeholders' pressures.

xi. European digital sovereignty

The central position of hyperscalers entails that the increase of the cloudification (i.e., the move of IT workload and data into the cloud) of the European economy including public services constitutes an increasing dependency on a few players.

As described in the 'European strategy for data', "*EU-based cloud providers have only a small share of the cloud market, which makes the EU highly dependent on external providers, vulnerable to external data threats and subject to a loss of investment potential for the European digital industry in the data processing market."*

This situation has not only led to competition concerns, but it has been also one of the reasons for a call to strengthening European digital sovereignty[172]. This has been done in a balanced approach aiming to mitigate the diverse risks while continue benefiting of the innovations and advantages of cloud services, including the ones offered by *hyperscalers*.

Along these lines, some of the recent EU initiatives, such as requirements to process data within the EU respond to this call and it is expected that digital sovereignty will continue being considered in any upcoming regulatory initiatives in this field.

The 'European Alliance for Industrial Data, Edge and Cloud', set up by the 'Member States Joint Declaration on building the next generation of cloud in Europe', has delivered a comprehensive 'Roadmap for the Next-Generation Cloud-Edge' that has been updated in 2023[173]. This roadmap identifies digital sovereignty as one of the priority areas for the development of cloud and edge services in the EU. In addition to the EU normative power,

[172] Digital sovereignty impacts all the elements in the value chain (hardware, software, data, infrastructure, etc.), some of them are out of the scope of this report.

[173] https://ec.europa.eu/newsroom/dae/redirection/document/97129

among many other proposals, this industry group suggests that digital sovereignty shall also involve the empowerment of users and the whole EU society (for instance, by enhancing the procurement capabilities of the organizations so that they can take more informed decisions and gain bargain power). They also call for the convergence of EU rules and a clearer framework of the enforcement capabilities of national regulatory bodies as a way to strengthen the implementation of the EU rules.

This duty to secure and protect sovereignty is becoming increasingly important as more governments embrace the cloud. In France, for example, since May 2021, the "cloud at the centre" doctrine has required the cloud to become the default hosting method for all government digital services[174].

These public administrations or organisations with a public service mission (local authorities, public services, companies, associations, etc.) organise, structure and facilitate the daily life of citizens. Their digital sovereignty therefore determines that of each individual user. This sovereignty must therefore be protected in the best possible way[175]. The adoption of cloud services by businesses must not therefore take place in the context of weak existing data protection frameworks, which raise sovereignty issues. This sovereignty must be protected in two ways: i) by limiting the dependence of these organisations on hyperscalers; and ii) by limiting the risks of transferring the sensitive data they use.

The DA could address these risks. For example, the interoperability and portability requirements for cloud services aim to increase supplier diversity by implementing measures to avoid lock-in. These requirements could therefore limit EU end-users‘ dependence on hyperscalers. In addition, on protecting and sovereignty in the cloud, it includes on the DA transparency obligations on international access and transfer of data, and on unlawful international governmental access and transfer of non-personal data.

Nevertheless, it seems essential to address sovereignty considerations in the long term giving priority to solutions to enhance EU Member States digital independence, in particular by establishing a reliable and sovereign digital infrastructure for the EU, as planned with GAIA-X. It also seems essential to implement monitoring or risk assessments of sovereignty issues in the cloud. In this respect, some Member States, such as France[176] and Germany, have introduced a national certification scheme for cloud service providers, which guarantees a certain level of security for data transfers. With this in mind, it will be relevant assessing whether these certifications meet the above objectives and the scope for their harmonisation within the EU.

[174] Cloud au centre: la doctrine de l'État. numerique.gouv.fr
[175] Cloud souverain: souveraineté et résilience, ou confiance? Cairn.info
[176] SecNumCloud pour les fournisseurs de services Cloud | ANSSI cyber.gouv.fr

xii. Sustainability

The European Climate Law[177] writes into law the goal set out in the European Green Deal to become climate-neutral by 2050, including an intermediate target of reducing net greenhouse gas emissions by at least 55% by 2030 (compared to 1990 levels). While cloud and edge services can enable more sustainable solutions across the markets, e.g., by sharing hardware resources (compared to often underused on premise hardware), concerns about the energy and water consumption and abiotic resources required by the data centres have arisen[178].

The 2020 EC Communication on Shaping Europe's Digital Future[179] fosters initiatives to achieve climate-neutral, highly energy efficient and sustainable data centres and transparency measures for ECN operators on their environmental footprint. In this context, the Energy Efficiency Directive[180] amended in September 2023, mandates the collection and publication of data which are relevant for the energy performance, water footprint and demand-side flexibility of data centres with significant footprint. Other related EU initiatives include: the inclusion of data centres in the EU taxonomy for sustainable activities[181], Green Public Procurement criteria, Ecodesign requirements on servers and data storage products[182] or the Code of Conduct for energy efficient Data Centres.

In addition, providers will have to engage in additional efforts to reduce their environmental impact not only to meet the EU standards and for the social welfare but also to decrease the costs related to the high consumption of resources[183]. Interesting initiatives are taken by Eurofiber in the Netherlands and AWS in Spain[184].

General elements related to sustainability considerations are already present in the EECC, as recalled in the External Study. Environmental and sustainability issues are key concerns shared by all, including BEREC. Thus, in the last years BEREC has been working on these matters and delivered different reports and studies regarding sustainability in the digital sector. In this regard, it would be worthwhile to continue to explore the issue by contributing to the development and improvement of environmental data collection and promoting the ability to carry out robust assessments of the environmental impacts of cloudification in the coming

---

[177] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R1119

[178] For instance, data centres water and energy consumption was discussed in the Dutch media https://www.datacenter-forum.com/datacenter-forum/data-centers-in-the-netherlands-could-lead-to-drinking-water-shortages

[179] https://commission.europa.eu/publications/communication-shaping-europes-digital-future_en

[180] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2023_231_R_0001&qid=1695186598766

[181] https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/eu-taxonomy-sustainable-activities_en

[182] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553786820621&uri=CELEX%3A32019R0424

[183] To support these efforts, the EC has elaborated a Code of Conduct for Energy Efficiency in Data Centres, https://joint-research-centre.ec.europa.eu/energy-efficiency/energy-efficiency-products/code-conduct-ict/code-conduct-energy-efficiency-data-centres_en

[184] Eurofiber is experimenting with separating the more energy consuming computing servers from the data warehousing. The location where the computing takes place is flexible and depends on the availability of sustainable energy resources (i.e. the location with most solar energy). Providers also experiment with waste energy that can be re-used. Instead of cooling with air, oil can be used to absorb temperature waste more efficiently. Microsoft planned its data centres next to greenhouses in the Netherlands. Eurofiber is testing to use its waste energy for city heating. AWS has recently built a data centre with its own windmill for energy supply.

years, in order to continue to integrate these considerations into regulation. To effectively monitor the sustainability of networks, it is also necessary to adapt the tools used to measure environmental impacts in the context of the migration of ECN/S to cloud services. To this end, consideration should be given to how NRAs could accurately assess both the CO2 emissions associated with the provision of ECN/S and the CO2 emissions associated with the provision of cloud services.

xiii. Digital divide

As the External Study notes, there is a risk that innovation and development of new services delivers benefit to some users while excluding others because of affordability. In this sense, as the study recommends, it is up to regulators to monitor these potential (new) digital divides by facilitating the implementation of a universal service (subject to its definition in case those new services are sufficiently widespread and relevant for society), promoting digital skills and addressing barriers to digital engagement.

8. Future Trends

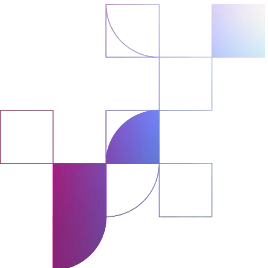
There are evident difficulties in anticipating the evolution of digital fast-evolving services. In the case of data processing services this difficulty is even greater as those developments (5G SA, cloud-based networks, or edge computing in particular as well as AI systems or quantum computing) are in an early phase of implementation by ECN/S operators. The market is still in a growing phase and, thus, not yet being mature and stable enough to allow the most reliable predictions.

As explained along the report and summarized in ANNEX I, the EU has been very active in the last years developing a vision for the EU cloud services environment, fostering public and private investment and putting forward binding regulation. Those initiatives aim to address bottlenecks and reshape the market making it more open and interoperable. However, the evaluation of the functioning of these, in particular, the latest DMA and DA Regulations, will only be possible in the mid-term (i.e., 5 to 10 years from now).

Taking into consideration of the caveats above, some trends for the upcoming years can be observed as follows:

i. The market will continue growing

Most EU businesses are still in the process of migrating on premise IT workload to the cloud and starting to explore the possibilities of new cloud-based services. According to Eurostat, only 41 % of EU enterprises used cloud computing in 2021 and most of this use was for less



sophisticated services such as e-mail and storage of files[185]. However, there was an increase of 5% compared to the previous year.

According to Gartner[186], by 2025, 51% of IT spending will have shifted from traditional solutions to the public cloud, compared to 41% in 2022. Almost two-thirds (65.9%) of spending on application software will be directed toward cloud technologies in 2025, up from 57.7% in 2022. In the case of edge computing, the infrastructures are still being deployed. The uptake of one of the key drives for edge computing, IoT services, is still low. Eurostat indicates that, in 2021, only 29 % of EU enterprises used IoT devices, mostly for keeping their premises secure[187]. However, use cases for edge computing are progressively gaining momentum. Virtual worlds, connected mobility, remote surgery, industry 4.0, etc. will require high and fast pacing investments in edge computing for EU to keep abreast of digital evolution and economic global competitiveness.

ii. Portability, switching and multi-cloud will become increasingly important

As users are currently moving into the cloud, some time will be required until changing or combining cloud providers is broadly undertaken. Moreover, the DMA and DA obligations in this regard will also require some implementation time until those are fully into force. Experience in the electronic communications sector shows that business customers tend to be less prompt to change providers than consumers[188]. This might be a factor limiting the use of these measures also in the case of cloud services.

iii. From ECS and cloud services bundling to tailored services

ECS and IT, including cloud services, are currently increasingly being provided as a bundle. In the coming future, network developments, such as 5G private networks, are able to create an environment fully customised to meet the needs of the specific use-case integrating cloud/edge and other IT services with network resources. This feature enables the join provision, not just as a bundle but as customized solutions, for instance, for vertical industries. Moreover, tailored offers (including IT, cloud/edge and connectivity elements) to meet customers' needs is perceived as opportunity for electronic communications' providers to differentiate their products and develop new value-added services.

---

[185] See e.g. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights

[186] https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending

[187] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_Internet_of_Things_in_enterprises

[188] The external Study on Communication Services for Businesses in Europe: Status Quo and Future Trends commissioned by BEREC indicates that the large majority of business users are satisfied with their electronic communication suppliers. https://www.berec.europa.eu/en/document-categories/berec/others/external-study-on-communication-services-for-businesses-in-europe-status-quo-and-future-trends

iv. Partnerships

The symbiotic relation between cloud, edge and ECN/S has favoured partnerships among different players to flourish all across the value chain[189]. However, the integration of the services and expansion of the providers into the other layers of service provision described above may raise the question regarding to what extent providers will continue relying on partnerships or will continue expanding to other areas for the provision of the service[190]. The feedback received during the interviews carried out for the elaboration of the report signals that partnerships will continue to be key in the coming years.

v. Cloud to edge continuum

The latest developments of cloud computing are leading to decentralization architecture with different levels from edge to fog to the central data centre. Integration requirements from the devices to the cloud going through the different levels of the edge has led to the concept of cloud continuum. Cloud continuum entails ubiquitous and seamless computing environments integrating all cloud resources and services (including private clouds and multi-clouds) supported by advanced connectivity. This advanced connectivity requires current ECN to be adapted to the provision of the cloud and edge services to serve ultra-low latency and reliable applications. This adaptation will be, in turn, enabled by the use of virtualized networks and NaaS network functions configuration. The cloud to edge compute continuum will require more significant efforts and progress in interoperability and orchestration but advances in this direction are expected to take place in the coming years.

vi. Further ECN transformation

The ECN architecture will have to be adapted and network management and orchestration optimized, coordinated and integrated with the edge and cloud to deliver the end-to-end connectivity in the cloud continuum. In the longer term, additional network architecture developments are expected. This is the case, for instance, of the Central office Rearchitected as a data centre (CORD) initiative'[191]. There are, however, still technical challenges to allow restructuring legacy networks into distributed micro data centres related to workloads

[189] BEREC's Report on the 5G Ecosystem develops on the different partnerships around the provision of 5G services.

[190] For instance, the 5G PPP Technology Board has elaborated in this regard in "Edge Computing for 5G Networks" (2021).

[191] In words of Manzalini and Marino "*5G will integrate fixed-mobile networks with highly distributed Cloud-Edge Computing facilities composed by (a limited number of) big-medium Data Centers (literally replacing current Telecommunications Central Offices) and a large number of small-medium Data Centers at the edge of the current infrastructure (i.e., in the access/distribution segments). (…) any resources, functionalities, capabilities will be provided/accessed/managed as pieces of services/applications through standard APIs, which will be made available, in a secured way, across the different levels of this future infrastructure. Clearly, in order to make this huge digital transformation possible and sustainable it will be necessary to evolve legacy networks and services infrastructures and the management and operations processes."* A. Manzalini and F. Marino, "Operating Systems for 5G Services Infrastructures: Convergence between IT and Telecommunications industry structures," 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), Porto, Portugal, 2018, pp. 1-5, doi: 10.1109/VTCSpring.2018.8417831.

portability between virtualized infrastructures and end-to-end orchestration that, as underlined by the authors, require further standardization efforts.

vii. Hyperscalers are expected to continue holding a central position

Cloud decentralization will require new edge nodes and other related deployments to approximate data processing nearer the users. Such developments have been perceived as an opportunity for different players to enter the market. In the case of ECN/S providers, the capillarity of the existing telecommunication networks may be a relevant advantage for edge deployment. Latest EU legislation (e.g., DA, DMA) imposes new obligations on cloud providers and in particular hyperscalers and has made a firm commitment on fostering open standards and interoperability to tackle current bottlenecks.

Those measures would facilitate opening the markets to new cloud providers entrants and the growth of existing ones. Nevertheless, despite those developments and the measures taken, hyperscalers are meant to continue holding a central position in the coming years and, in many cases, be an unavoidable partner for many of the players in the ecosystem for the following reasons: i) cloud and edge services are not substitutes but complementary; ii) even in the case that new players step into the cloud business by investing on the edge, the provision of NaaS or the commercialization of cloud and ECN/S integrated offers, they will still have to rely on partnerships with cloud providers including in most cases the hyperscalers; and iii) the competitive advantages of hyperscalers described in chapter 4 are not likely to change in the mid-term. Thus, they will remain as a predominant player for the provision of the services.

ANNEX I. EU initiatives related to cloud/edge

NON- EXAUSTIVE OVERVIEW OF EU INITIATIVES RELATED TO CLOUD/EDGE[192]	
EU ACT	**MAIN TOPICS FOR CLOUD/EDGE**
EC Communication: Unleashing the Potential of Cloud Computing in Europe[193] (2012)	Defines 3 lines of actions for Europe to reap all the benefits of cloud computing: (i) Standardisation and certification actions; (iii) Safe and fair contract terms and conditions and (iii) a European Cloud Partnership to drive innovation and growth from the public sector.
Regulation: General Data Protection Regulation (GDPR)[194] (2016)	Establishes the rights to the free movement of personal data within the UE and personal data portability. It also regulates the transfers of personal data to third countries or international organisations[195]. The general rule is that international transfers of personal data are not allowed unless certain safeguards are met.
Regulation: Free flow of non-personal data (2018)[196]	Establishes the right to the free movement of non-personal data within the UE. Encourages the development of EU codes of conduct to, among others, facilitate switching, data portability and interoperability of data processing services[197].
Directive Open Data (2019)[198]	Open data and re-use of public sector information
EC Communication: A European strategy for data[199] (2020)	Aims for a single European data space complemented by sectoral data spaces in strategic areas (e.g., mobility). The Data Strategy defines actions on 4 pillars: (i) cross-sectoral governance framework for data access and use; (ii) investments in data and infrastructures for hosting, processing and using data, interoperability; (iii)

[192] Among the initiatives that have not been included are those related to cybersecurity (e.g., NIS 2 Directive, the Critical Entities Resilience (CER) Directive, or the Cybersecurity Act) or illegal content liability under the Digital Services Act (DSA) as hosting services.
[193] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0529
[194] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1688727547160
[195] Cloud service providers shall abide with these rules as data controllers or processors.
[196] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807
[197] The EC facilitated the establishment of a multi-stakeholder organization, SWIPO (Switching Cloud Providers and Porting Data) to foster these codes of conduct. https://swipo.eu/
[198] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024
[199] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066

	empowering individuals, digital skill and capacity building for SME; (iv) EU data spaces in strategic sectors and domains of public interest. Relevant measures related to cloud services include: (i) the provision of data infrastructures, data spaces and federated cloud infrastructures[200]; (ii) the delivery of the Data Act; (iii) EU Cloud Rulebook[201]; (iv) a European cloud services marketplace.
Member States Joint Declaration: On building the next generation of cloud in Europe[202] (2020)	This Declaration builds on the idea of a European cloud federation to supply Europe with secure, energy-efficient and interoperable cloud service provision, based on a set of common technical rules and norms (the EU Cloud Rulebook) and an ambitious investment plan[203]. The setup of a European Alliance for Industrial Data and Cloud is foreseen to support the European cloud federation.
EC Communication 2030 Digital Compass: the European way for the Digital Decade[204] (2021)	Defines 2 key policy objectives related to cloud/edge to be met by 2030: (i) 75% of European businesses should use cloud-edge technologies for their activities and (ii) the deployment of 10,000 climate-neutral and highly secure edge nodes.
Regulation Digital Markets Act (DMA) (2022)	Cloud services are classified as "Core Platform Services" (CPS) under the DMA. This implies that providers that meet certain conditions and, thus, qualify as "gatekeeper" shall abide with a number of asymmetric obligations aimed to enhance market contestability of the market.
Regulation Data Governance Act (2022)[205]	Regulates: (i) re-use of public sector data (complementing Open Data Directive); (ii) data intermediation services including interoperability obligations; (iii) data sharing for altruistic purposes; (iv)establishes the European Data Innovation Board.
Regulation Data Act (2023)[206]	Includes switching and interoperability obligations on data processing services (i.e. encompassing cloud, edge and

[200] In this regard, the Strategy proposes cooperating with MMSS initiatives such as Gaia-X. Gaia-X, the European Association for Data and Cloud, was initially launched with the support of the French and German Governments in 2019.
[201] The cloud rulebook will gather all the different applicable rules (including self-regulation) for cloud services. The European strategy for data indicates that, in a first instance, the rulebook will offer a compendium of existing cloud codes of conduct and certification on security, energy efficiency, quality of service, data protection and data portability.
[202] https://ec.europa.eu/newsroom/dae/redirection/document/70089
[203] The Declaration estimates a 11billion€ annual investment gap for cloud in the EU.
[204] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0118
[205] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767
[206] http://data.europa.eu/eli/reg/2023/2854/oj

	any other similar services such as fog computing) providers.
Draft Regulation Artificial Intelligence Act[207]	Aims at facilitating the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation by ensuring that AI systems in the EU are human centric, safe and in line with the EU law as well as providing legal certainty to facilitate investment and innovation.

[207] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

ANNEX II. Acronyms

AI – Artificial Intelligence

APIs - Application Programming Interfaces

AWS - Amazon Web Services

BBU - Base-band Units

BSS - business support

B2B - Business to Business

CAPs - Content and Application Providers

Capex – Capital expenditure

CDN - Content Delivery Networks

CISPE - Cloud Infrastructure Service Providers in Europe

CNF - Cloud-native Network Functions

C-RAN - Cloud RAN

CPaaS - Communication Platform as a Service

CPRI - Common Public Radio Interface

CPS - Core Platform Service

CU - Centralized Units

C-RAN - Cloud RAN

DA – Data Act

DMA - Digital Markets Act

DNA - Digital Networks Act

DU - Distributed Units

EC – European Commission

EU – European Union

ECN - Electronic Communication Networks

ECS - Electronic Communication Services

E/WBI - East and Westbound interface

GDPR - General Data Protection Regulation

IaaS - Infrastructure-as-a-Service

IoT – Internet of Things

IPCEI - Important Project of Common European Interest

ISP - Internet Service Provider

ISVs- Independent Software Vendors

IT - Information Technology

MEC - Multi-Access Edge Computing

ML – Machine Learning

NaaS - Network as a Service

NBI - Northbound Interface

NFV - Network Function Virtualisation

NIST - National Institute of Standards and Technology

NRA - National Regulatory Authority

OCA- Other Competent Authority

Opex - Operational expenditure

OS - Operating System

OSS - operation and orchestration

PaaS - Platform-as-a-Service

QoE - Quality of Experience

RAN - Radio Access Network

RRH - Remote Radio Heads RRH

RU - Radio Units

R&D- Research and Development

5G SA – 5G Standalone

SaaS - Software-as-a-Service

SBA - Service-Based Cloud Architecture

SBI - Southbound Interface

SDI – Software Defined Infrastructure

SDN - Software Defined Networking

SD-WAN - Software Defined Wide Area Network

SWIPO - Switching Cloud Providers and Porting Data

UPF - User Plane Function

VM – Virtual Machine

VR – Virtual Reality

vRAN - Virtual RAN

V2X - Vehicle-to-everything

ANNEX III. Interviews with stakeholders

For the elaboration of this report, BEREC hold informal exchanges with the following organizations:

Analysys Mason	CISCO	Google
Akamai	CISPE	OVH Cloud
AT&T	Colt	Telefónica
Capgemini	Deutsche Telekom	VMWare
CCIA	ECTA	
Cellnex	Gaia-X	