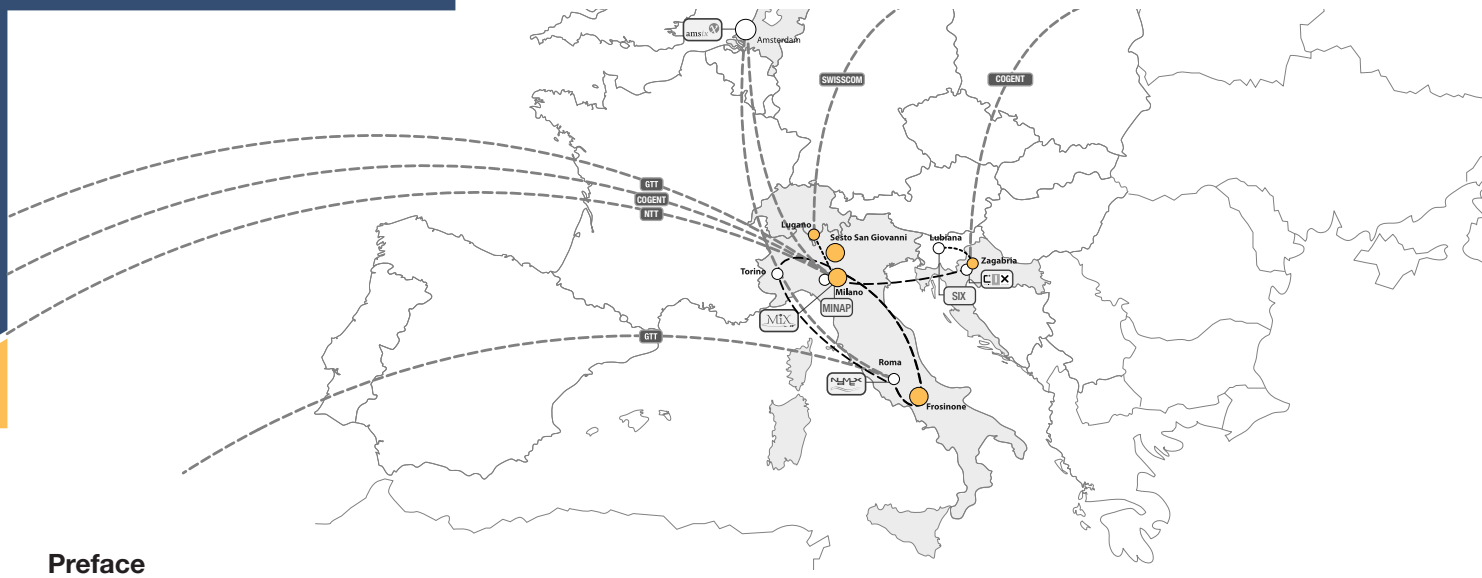
THE REACHABILITY OF DATA: A LEGAL PERSPECTIVE

Research by:
Innocenzo Genna
Eugenio Prosperetti

With the collaboration of:
Giulio Pascali
Davide Tuzzolino

sponsored by DOMINION HOSTING HOLDING



Preface

Nowadays, we talk a lot about data: we know how to collect and read it in the right way for every company, increasing efficiency, improving processes. But what is behind it? Behind the data, there are people and companies, but these are the fundamental and critical assets at the same time and the responsibilities of those who are called upon to host and manage them: the cloud operators.

Seeweb has always been particularly sensitive to data management that follows the European criteria of attention to privacy, which is increasingly crucial in the multicloud era that has been much talked about recently as a solution to technological or lock-in problems.

On the other hand, the implications on data protection and privacy following the adoption of the multicloud paradigm are less clear: are all cloud providers the same from this point of view, so much so that they can be interchanged with serenity as easily as they can at the technological level? The answer is no, and indeed the risks are complex and cannot be ignored.

Today, all cloud providers promote themselves as safe havens for their customers' data, but there is one relevant issue: in a global context where more than half of European companies and organizations are adopting US cloud systems (regardless of where the data centers are located) to host their strategic data, what do we need to know?

The Privacy Shield was invalidated on 16 July 2020 when the European Court of Justice declared that the protection of personal data offered by the EU-US Privacy Shield regime was inadequate. In light of the GDPR, there do not appear to be adequate safeguards to protect European data in relation to the US government's surveillance programs (one thinks of the datagate and the investigation and intelligence activities carried out by the government agency NSA). Since then, the transfer of data to operators subject to US law takes place under the responsibility of those who implement it in a scenario where Europe considers it illegitimate.

Thanks to the work of experts Eugenio Prosperetti and Innocenzo Genna, this whitepaper gets to the bottom of a complex issue, poses clear questions - and offers answers.

It provides the reader with an insight into the scenarios and developments that can arise when companies entrust their information assets to non-European players. It also addresses the unprecedented issue of the "legal reachability" of data, which remains even if the US provider's data centers are located in any EU state.

Antonio Baldassarra
CEO Seeweb

THE REACHABILITY OF DATA: A LEGAL PERSPECTIVE

Research by:
Innocenzo Genna
Eugenio Prosperetti

with the collaboration of:
Giulio Pascali
Davide Tuzzolino

The subject of this Study is the so-called "legal reachability" of data.

The legal notion of "reachability" was recently introduced to indicate the possibility for a subject to access and dispose, in a legitimate manner, of data stored in a cloud system. However, it is a notion that can be declined at various levels: on the one hand, there is "reachability" for the original data owner user, as well as for those who may acquire certain rights in the context of the cloud service; on the other hand, there is a further form of "reachability" of data by entities - typically government institutions or public authorities - who, in the exercise of their functions, may have an interest in accessing data located in a cloud.

In fact, data, once outsourced, become "reachable" by virtue of a complex patchwork of legal rules from different sources (international, European and national) and contractual provisions, whose overall weight and articulation are not indifferent for the cloud strategy of any organization, be it cloud provider or customer.

The issue of "legal reachability" is thus aimed at assessing, in practice, the accessibility and availability of data in a globalized economy, in order to assess the risk arising from the possibility that foreign government authorities, including non-European ones, may access or prohibit access to data placed in the cloud by virtue of authoritative powers, or even order their destruction, for instance following an embargo or for reasons of national security.

The Study takes particular account of the role of US operators in the European cloud sector, both because of their preponderant market share held by them in Europe [1], and due to the recent implications arising from the annulment of the Privacy Shield regime by the European Court of Justice.

1 Among the most recent data, see Synergy Research Group, First quarter 2020,
http://www.globenewswire.com/NewsRoom/AttachmentNg/5d1edd1e-dc3c-4847-9fc0-23a5e0eb20d5/en

Research summary

When data placed in the cloud are of particular importance, e.g. personal data or business data or data of economic importance, the choice of the cloud provider must be carefully considered. It is not simply a matter of evaluating the economic and technological offer proposed by the operator, but also of considering the fate that data entrusted in the cloud may have in the face of coercive measures by governmental or judicial authorities, which could sanction access, prohibition or even destruction. This is the issue of data reachability in the cloud, which is the subject of this Study.

In making this assessment, one must take into account the legal system that governs the overall processing and accessibility of the data covered by the cloud contract. In a purely European context, i.e. with cloud providers and servers within the EU, the data of a European citizen or company appear to be substantially safe due to the robust safeguards provided by EU legislation, primarily the GDPR.

However, it is also necessary to consider the nationality of the cloud provider, since this may imply the jurisdiction of third and non-European countries that may consider themselves authorized to intervene on their own companies, also with reference to data of European citizens stored in servers located in Europe; therefore, the physical location of the servers does not mitigate the requirements deriving from the nationality of the cloud provider. The most common case, i.e. that of the US cloud provider, requires assessing the applicability of US legislation, and in particular the Cloud Act, which may vary depending on the agreements made with the various European States. With other nationalities and with countries whose legislation appears to be very distant from the European one, for instance China and other Asian countries, the case appears even more complex and delicate, so that the reachability of data entrusted in the cloud must be carefully assessed.

The prior assessment of the applicable legislation and jurisdiction is therefore a necessary and indispensable step, alongside economic and technological considerations. The uncertainties and risks resulting from this assessment can however be compensated by the preparation of contractual models and policies that regulate in advance and in detail the behavior that the cloud provider must adopt in the case of measures of authorities of third countries, with reference to the accessibility and storage of data.

INDEX

Chapter I - Cloud and data

Chapter 2 - Property, ownership and other data rights

Chapter 3 - The legal framework governing data reachability in the cloud

Chapter 4 - Public authorities' intervention in data reachability

Chapter 5 - Conclusions

CHAPTER I
CLOUD AND DATA

1.1 Definition, models and diffusion of cloud services

Cloud definition

There is no single definition, in legal, technical or commercial language, of cloud or, as we say in Italian, of "computer cloud". Indeed, the ability of the cloud to adapt elastically to market needs suggests the use of a flexible notion that is as all-encompassing as possible, even at the risk of some inaccuracies.

Given this premise, the cloud can be defined in the first instance as a network of servers, located anywhere and connected to each other, which working as a single ecosystem allow a wide range of activities to be performed in a scalable and elastic manner that would otherwise have to be performed with their own local hardware and software resources. This includes activities such as storing and managing data, running applications, providing computing power, distributing content or services, including streaming video, webmail, software or social media platforms. The cloud also enables activities that could not be performed locally at all, such as working together on the same platform from different locations and accessing, with relatively powerful and small computers and also on the move, to very large databases, powerful computing resources and artificial intelligence systems.

In line with the above, the Agency for Digital Italy (AgID), defines the cloud as *"a model of IT infrastructure that allows for the availability, via the Internet, of a set of computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly delivered as a service. This model makes it possible to drastically simplify the management of information systems, transforming physical infrastructures into virtual services that can be used according to the consumption of resources"*[2].

The notion of cloud becomes even clearer if one stresses the advantages of using this IT and organizational model over traditional hardware solutions. The cloud in fact allows:

- access to applications from any device and in any location, via the Internet or dedicated connectivity;
- significant savings in software usage, thanks to the possibility of paying for cloud resources on a pay-per-use basis, i.e. based on consumption, thus avoiding the high initial fixed investments involved in purchasing infrastructure and licenses;
- reducing data center costs (rent, electricity consumption, maintenance and cleaning, security, backup);
- greater flexibility and lower costs when testing new services or making changes to them;
- continuous updating of infrastructure and applications;
- greater security[3].

Cloud models

Within the overall definition of cloud, various models can be traced, depending on the distribution of cloud resources chosen by companies or on the macro-types of services that can be provided. These subdivisions, although technically complex, always reflect the basic concept, which identifies the cloud as a network of remote servers whose various services are accessible via telematic networks, which can be managed and offered on the market by different actors and providers, and provided on a contractual basis.

With regard to the infrastructure and distribution of cloud resources, the market currently identifies 4 main organizational models:

2 Definition set out at https://cloud.italia.it.
3 Cloud-based data management can offer the possibility to host data in infrastructures with levels of security otherwise inaccessible to small and medium-sized businesses/professional offices, and managed by specialized personnel.

- The public cloud, which operates through the sharing of global resources and offers services to the public via the Internet or dedicated connectivity;
- The private cloud, a cloud model in which services are offered only to pre-identified users and not to the general public; it may be based on private servers or on large servers that are appropriately configured to separate the various cloud users (normally using Infrastructure-as-a-Service and Platform-as-a-Service models) or, again, offer services over a private internal network hosting the resources locally;
- The hybrid cloud, which shares services between public and private clouds depending on the purpose;
- The community cloud, where the cloud infrastructure is set up to provide cloud services to a specific community of organizations that have shared requirements and objectives.

From the point of view of the services that can be used through the cloud, commercial practice tends to distinguish three main types:

- Infrastructure-as-a-Service (IaaS), i.e. the provision of a physical technological infrastructure in virtual form as a service for accessing (also on-demand) IT resources such as networks, memory and servers remotely using appropriate software and Application Programming Interfaces (APIs), in a scalable form and without the need to purchase hardware and licenses;
- Platform-as-a-Service (PaaS), i.e. the provision as a service of a computing environment for testing, developing and managing applications;
- Software-as-a-Service (SaaS), i.e. services provided through the processing of data using software applications installed and running on the cloud provider's servers, and accessible via the Internet using different types of devices (Desktop, Mobile, etc.).

The technical definitions of the cloud model and the specific properties of the services can be consulted at NIST[4]

The cloud in Italy

In Italy, cloud services have spread fairly recently. The spread was initially conditioned by various factors such as the size of companies and their growth characteristics, the need or otherwise to have data distributed across the territory, and the availability of internal IT capacity. However, the market is now growing strongly, partly due to the tremendous boost provided by the Covid-19 pandemic in 2020, which required companies and communities to reorganize their activities and processes [5] in an agile way. By the end of 2020, 59% of Italian businesses were using cloud computing services[6].

According to the estimates of the Cloud Observatory of the "Politecnico di Milano"[7], in 2020 the Italian cloud market reached 3.34 billion euros, up by + 21% compared to the final balance of 2019, equal to 2.77 billion euros. In terms of absolute spending, the top three sectors in terms of relevance are Manufacturing (24%), Banking (21%) and Telco/Media (15%).

The most popular cloud services in Italy are the following:

-IaaS: includes cloud storage, cloud backup and synchronization, website hosting, cloud drive, virtual server services, including IBM Cloud, Google Cloud, Amazon AWS, Seeweb Cloud Server, Aruba, Irideos, etc.

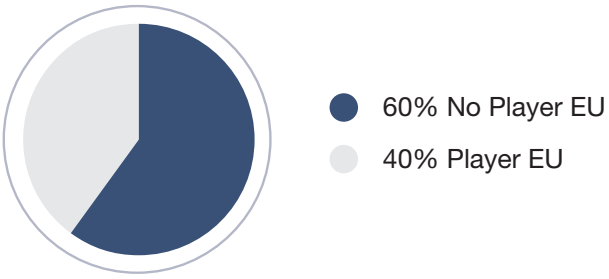
- PaaS services: this is a very fragmented market in which Amazon, SAP, Google, Oracle, Microsoft and IBM, among others, are active.

4 National Institute of Standards and Technology, US Department of Commerce; The Nist Definition of Cloud computing, Special Publication 800-145, September 2011. Available at the following link
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
5 The "leap forward" that occurred in Italy due to Covid is well represented by Eurostat statistics, Cloud computing - statistics on the use by enterprises, 19 January 2021.
6 Eurostat data: Use of cloud computing services in enterprises, 2020.
7 2019-2020 edition of the Cloud Transformation Observatory of October 2020; see the press release accessible at the following link: https://www.osservatori.net/it/ricerche/comunicati-stampa/cloud-italia-mercato-2020.

- SaaS processing services: includes extremely diverse services such as email accounts, operating systems (e.g. GSuite and Office 365), e-invoicing services from providers such as Infocert, Aruba, cloud-based office management systems such as Zucchetti and Team System, as well as popular services such as Dropbox, Onedrive, SugarSync, Google Drive, ICloud to name but a few.

According to data from the Ministry of Innovation, 60% of the Italian cloud market is supplied by non-European operators[8].

EUROPEAN CLOUD MARKET



Percentage use of European and U.S. cloud operators from Ministry of Innovation data

The cloud and the Italian public administration

The Three-Year Plan for IT in the Public Administration [9], adopted as part of the "Strategy for the Digital Growth of the Country"[10], has envisaged a strategy for the adoption of cloud computing in the Public Administration that is divided into three main elements:[11]

- the Cloud First principle according to which PAs must, as a matter of priority, adopt the cloud paradigm (in particular SaaS services) before any other traditional technological option, normally based on housing or hosting;
- the PA cloud model, i.e. the strategic model consisting of infrastructures and services qualified by AgID[12] on the basis of a set of requirements aimed at ensuring high quality and security standards for PA. In accordance with this model, a special platform has been created, the AgID Cloud Marketplace, which makes it possible to view the details of each service, highlighting the characteristics, cost and service levels declared by the supplier. PAs can thus compare similar services and decide on the most suitable solutions according to their needs.[13]
- the cloud enablement programme, i.e. the set of activities, resources and methodologies to be put in place to enable public administrations to migrate and efficiently maintain their IT services (infrastructure and applications) within the PA cloud model.

As of 1 April 2019, Public Administrations can only acquire IaaS, PaaS and SaaS services qualified by AgID and published in the Catalogue of qualified PA cloud services.

After an initial stalemate due to the difficulty of managing at an individual level the complexities of tenders for this "immaterial" type of services, the P.A. cloud market has taken off and is currently characterized by the provision of services through the CONSIP tender called "SPC Cloud". This model of public tender has awarded, as provided for in the above-mentioned Three-Year Plan, in the form of framework contracts with open and compulsory adhesion by the Public Administrations, four "lots" (categories) of cloud services in

8 Speech by Minister Paola Pisano, at the Gaia-X Summit online, 19 October 2020, available at the following link here: https://innovazione.gov.it/assets/docs/2020-11-19-intervento-ministra-pisano-a-gaia-x-summit.pdf.
9 Adopted by DPCM of 17 July 2020 and available at the following link: https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_l_informatica_nella_pa_2020_2022.pdf.
10 Version adopted in 2016, and following comments from the European Commission, and available at the following link: https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf.
11The 3 elements of the strategy are available at the following link: https://cloud.italia.it.
12 See AgID Circulars No. 2 and No. 3 of 9 April 2018. See also: https://cloud.italia.it/marketplace/.
13 The Marketplace also indicates how a specific service can be acquired by an administration by referring to the available procurement tool (the www.acquistinretepa.it portal) to proceed with the acquisition.

favor of the P.A.[14]

The arrival of global cloud providers, and in particular the US ones, has contributed to the growth of the Italian market and the automation of public administration processes. (as well as private individuals). At present, these global operators are well present in the Italian cloud services scene, although they are more active towards private individuals than towards the P.A., since the SPC tender entails complex contractual and administrative constraints specific to the winners of the above-mentioned lots. However, even in the private market, global cloud providers tend to adopt a model that sees them side by side with local partners, since the contractual models adopted by these international operators are highly standardized and difficult to adapt to local charges and conditions, as well as to the assumption of risks towards local public or private entities (e.g. provision of sureties, negotiation of specific contracts that envisage rights of verification or obligations to manage the cloud infrastructure ad hoc, penalties, etc.). Global cloud providers, therefore, prefer to be "intermediated" and provide a standard service, leaving any specificities and burdens required by the individual project to be contracted with a local reseller.[15]

It should also be remembered that the recent National Recovery and Resilience Plan [16] (the so-called Recovery Fund - Next Generation EU) under discussion at the time of writing, which provides for the creation of an Italian Public Administration cloud to be developed in line with the EU project "Gaia X". The project envisages the replacement, in an organic manner, of the local CEDs throughout Italy, standardizing and making efficient the storage and processing of the Italian Public Administration's data assets.

1.2. Data, information and related categories

For the purposes of this Study, it is necessary to clarify what is legally meant by "data", a term that normally covers signs, words and images transmitted by bits, and whether the latter, the bits, also have any legal relevance. It must also be established whether and on what grounds data should be distinguished from information.

Bits

Bits are the result of the conversion of human-intelligible data into electromagnetic pulses using a binary code. The binary code is based on the use of only two signs, 0 and 1, corresponding to two electrical states, which are called bits, term resulting from the binary digit crasis. Ordered sequences of bits make it possible to display representations (graphic signs, photos or moving images) on the computer screen.

The legal value of bits is debatable depending on whether one approaches it in the field of computer science (i.e. as a simple binary digit) or in the field of information theory (i.e. as the defined unit of measurement of the minimum amount of information). For the purposes of our Study, bits assume legal value only to the extent that they come, through a coding system, to represent ideas or concepts that are legally or economically relevant: in this case, we shall speak more properly of data or information. Bits that do not have this representational capacity are not relevant for the purposes of this Study, although they may still have legal relevance for other purposes (e.g. cybersecurity).

Data

The concept of data and its regulation in law is fundamental for the purposes of our Study, since the concrete contractual and regulatory structure of the cloud relationship is certainly influenced by the view of what constitutes "data" capable of producing legal effects in the system regulating the relationship between client

14 See https://www.consip.it/attivita/gara-spc-cloud-disponibile-la-documentazione and thematic websites of awarded framework contracts: lot 1: https://www.cloudspc.it/ lot 2: https://www.spc-lotto2-sicurezza.it/ lot 3: www.spclotto3.it lot 4: www.spclotto4.it.
15 Beyond the mentioned contractual tasks towards the PA, the main purpose of these local resellers is to provide sales force on the territory and ensure the integration of services (both cloud and others). However, there may be little possibility for these small resellers to influence the policy, technology and governance of cloud services (e.g. security policies, territorial distribution of data, configuration of services), which remain mainly in the hands of the global operator. This should be assessed on a case-by-case basis. It is also worth noting, in the national context, indicating the growing importance of national realities capable of interacting with large cloud operators (in this case Google), the very recent establishment of the new company Noovle Spa dedicated to cloud enabling activities into which the Telecom Italia group's data center network has converged.
16 See http://www.politicheeuropee.gov.it/it/comunicazione/approfondimenti/pnrr-approfondimento/.

and provider.

Data are representations intelligible to man and can be defined, in particular, as *"original, i.e. uninterpreted, representations of a phenomenon, event, or fact, made through symbols or combinations of symbols, or any other form of expression linked to any medium*.[17] This representational capacity derives from the encoding that makes it possible to convert - in the case of data in electronic format - bits into symbols, images and sounds.

The data are of unquestionable legal and economic importance and as such, are subject to specific protection in accordance with the applicable rules.

The main regulation enshrining such legal effects is the European regulation on the "electronic document", introduced by Regulation (EU) 2014/910[18] (so-called "EIDAS Regulation"). According to Article 43 of the Regulation, "data" contained in an electronic document cannot be denied legal effects on the ground of its electronic form. Therefore, a court cannot refuse to take into account electronic documents and the data contained therein, and must examine their merits.

The electronic document is defined by the EU regulation as: *"any content stored in electronic form, in particular text or sound, visual or audiovisual record"*. Consequently, under EU law, the issue of reachability concerns those data that meet the definition of electronic document just mentioned, as they can be the subject of legal measures. To complete the European regulatory framework, mention should also be made of Regulation 2016/679 on the protection of personal data (the so-called GDPR) as well as Directive 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offenses or the execution of criminal penalties[19] ; nor should we forget the rules governing intellectual property on the data themselves and, as will be discussed in the following paragraphs, the new provisions concerning the circulation, access and portability of "non-personal" data.

> *"A significant portion of the cloud market is in the hands of large US players, hence the need for a thorough understanding of the legal aspects beyond the physical location of their data centers."*

In non-EU jurisdictions such as the US, the definitions of electronic documents tend to be broader and less detailed. For example, in the USA, the Uniform Electronic Transactions Act (UETA) defines *"electronic record"* as *"a record created, generated, sent, communicated, received, or stored by electronic means"*, thus indicating any possible format and content.

In this respect, it should be recalled, however, that in the US there is no federal legislation on the protection of "data" or "personal data" based on a model comparable to the European one. The protection is mainly indirect, as it is based on consumer protection rules, e.g. through the Federal Trade Commission Act of 1914, but there are also individual state laws (e.g. California) protecting personal data. The consequence of this is that unlike the EU, which is based on a more rigid and guaranteeing system, in the USA, the simple collection of data, even massive, is not, as a rule, subject to prior authorization (i.e. the consent of the data subject), while it is only the use of the data that is regulated, case by case and according to the territory in which it takes place.

Information

Data should in principle be distinguished from information, since information is the result of a particular temporal and spatial sequence of data that makes possible a process of interpretation that is meaningful for the recipient - whereas not all data can hold such "information content", but, as mentioned above, only those that are able to express it are legally relevant. However, the legal disciplines mainly refer to the concept of data/information as a whole, rather than giving importance to the distinction between the two concepts. For

17 Definition taken from http://www.dei.unipd.it/~dinunzio/fdi-2014-2015/04_dati_informazioni.pdf .
18 Regulation (EU) 2014/910 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Art. 3 para. 35.
19 See chapter 2 of the Study.

example, the Open Data Directive considers data as a synonym of document[20], while the recent proposal of the Data Governance Act also adopts an overall definition whereby data is defined as *"any digital representation of acts, facts or information"*[21]. Also, the GDPR, referring to personal data, adopts an overall definition of data and information.[22] Therefore, in view of all this, for the purposes of our Study, it will not be necessary to systematically distinguish between data and information, except where required by specific circumstances. Therefore, when we refer to the concept of "data", we shall also mean data having an interpretable information content, i.e. also information.

The term information is also often used in legal language in conjunction with "confidential" or "reserved" to define that particular type of data that forms part of the company's assets and is made the subject of special confidentiality obligations in the course of a contractual relationship. In this sense, the term "information" indicates both personal and non-personal data and refers to the unambiguousness of the ownership/provenance of the set of data.

Categories of data: personal and non-personal

Although the concept of data is strongly linked to the notion of personal data under the GDPR, being the legal corpus that first enhanced its legal value in a general sense, this is not the only meaning of data relevant for the purposes of our Study. In fact, data may also be non-personal, i.e. not associated with an identified or identifiable person on the basis of the data. The regime and circulation of non-personal data is subject, *inter alia*, to the aforementioned legislation set out in Regulation (EU) 2018/1807[23], which concerns the accessibility and portability of non-personal data and which will be better described in Chapter 4.

Non-personal data can be qualified as follows:

(i) data that do not originally relate to an identified or identifiable natural person, e.g. statistical, meteorological, industrial or commercial data. Among these data, data from the devices and robotics that make up the infrastructure of the Internet of Things (e.g. traffic data, weather) and data relating to companies (commercial data such as customer lists, sales and cost data, trade secrets not yet covered by IP, know-how, contractual texts, source code, patents under study, etc.) take on an important role;

(ii) data that were initially personal data, but were later rendered anonymous as they underwent a process of anonymization;

(iii) mixed data, i.e. a set of both personal and non-personal data (e.g. data from a company's tax or public records, indicating name and other information on managers).

The cloud is in fact not composed of personal data only, and in this sense, throughout the Study, where appropriate, we will distinguish "non-personal and corporate data" from "personal data", while the term "data" without further specification will mean both.

1.3. The data "localization"

The concept of data localization has to deal with the intangible nature of data, and therefore does not correspond to the same concept used for physical goods. With regard to data, this concept must take account of their composite nature: on the one hand, the electronic nature of the bits, on the other hand, the software that allows these bits to be controlled and, ultimately, to produce, from the bits, a result that is intelligible to the recipient (through encoding).

20 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019, Articles 1 and 2.
21 Article 2 (1) of the "Proposal for a Regulation of the European Parliament and of the Council on European data (Data Governance Act) {SEC(2020) 405 final}: *"data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording;"*.
22 Article 4(1) of the GDPR in relation to the definition of personal data: *"«personal data»: any information relating to an identified or identifiable natural person («data subject»)"*.
23 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free movement of non-personal data in the European Union.

Localization and bits

The electronic nature of bits complicates the classic concept of localization. In fact, the bits are localized in hardware devices connected to servers on which the applications are installed and which perform the functions of calculation and processing. For the sake of simplicity, however, it is customary to say that the bits are localized in the servers, and this Study will also adopt this statement, although we know that it is a simplification.

However, data can be fragmented (through so-called striping) and its bits distributed across several servers, which may be located in different data centers and even in different countries (e.g. to provide efficient backup). Moreover, in order to avoid problems arising from the failure of a single server, a cloud provider may choose to use redundancy policies whereby the same data is at the same time fragmented in several servers, also located in different countries, and therefore its exact location cannot be exactly determined. Allocation and distribution of bits/data can also vary over time, even many times a day, hour or even minute, as a result of cloud provider management policies. Data centers and servers may also belong to different operators than the cloud provider, a quite common practice to allow the elasticity of the cloud service. The contractualization of such cases can be complex, ranging from co-location at external data centers to outright outsourcing.

In spite of the complexity just described, the cloud operator should in principle always be able to know where the data are located, i.e. on which servers the relevant bits are distributed at any given time, since such knowledge is necessary, for instance, to be able to fulfill a judicial request. This knowledge of the location by the operator does not, however, generally correspond to the possibility of keeping its customer informed of where the data reside, except in general terms, by indicating, for instance, the geographical macro-area in which the servers where the data will be managed are located.

> *"The legal location of data is a fundamental concept that governs data transfer. Today, except in strictly defined cases, with the GDPR, data cannot be transferred outside of the EU."*

Localization and software

The encoding and IT processes that resolve electrical impulses into intelligible content add another layer of complexity. The one who controls the software needed to govern these processes and the governance rules of the system that manages their localization and security is the real dominus of the data, but he may be a subject distinct from the cloud provider or the owner of the servers, or even from the party with whom the data owner has entered into a contractual relationship (the intermediary, the reseller, the aggregator, etc.). Therefore, the concept of localization cannot disregard this legal complexity. Thus, for the purposes of the GDPR, the responsible entity for the data is the "owner" (and subordinately the "controller"), whereas, under e-commerce law, the entity responsible is the one who manages the website or an online platform and who therefore has the tools to carry out the removal of content declared to be unlawful. Therefore, in some circumstances, the control over data exercised, through software programs, by a cloud provider providing a SaaS service may be more penetrating, in terms of effectiveness, than that of their effective owner, i.e. the customer.[24]

The legal data localization

The concept of data localization is therefore complex and, for legal purposes, must take into account both the location of the servers and the location of the entity operating the software that controls the data. The applicable jurisdiction must therefore take both factors into account, depending on the purpose pursued. In a liability case, the location of the owner/controller is decisive, but in order to execute a seizure (e.g. to block

24 Interesting is the Italian rule provided for in Article 64 paragraph 2-quinquies of the CAD (Digital Administration Code approved by Legislative Decree 82/2005 subsequently amended and supplemented) which provides for the exemption of liability arising from the general obligation to monitor activities on one's own websites where access is provided with the SPID digital identity system. This is because in this case the users are identified with certainty and therefore the activities carried out on hosted sites are ascribable with certainty to identified users and in no case fall to the hosting provider.

a website), the location of the servers and, before that, the registered office of the controller/processor in charge of managing them, is also crucial.

The legal localization of data is also a key concept for data transfer disciplines. Data subject to the scope of the GDPR[25] cannot be transferred outside the EU except in strictly defined cases, while in the case of non-personal data, Regulation 2018/1807 provides that *"data localization obligations are prohibited unless they are justified for reasons of public security while respecting the principle of proportionality"*.

Encryption

Encryption, i.e. the process of ensuring data confidentiality through the use of private keys, must also be considered in the context of data control processes. In the context of cloud services, encryption is normally provided for data transmission and storage, but not for the processing and calculation phase, which must instead take place in plain text because the data must be "available" to those who process it (e.g. to be subject to enrichment that makes it suitable for feeding an artificial intelligence system).

Providing end-to-end encryption is still in part a complex process to manage from a technological point of view, and moreover unsuitable for securing the totality of the technological steps involved in cloud services because, as mentioned, some of them involve precisely the sharing of data between customer and cloud provider.

However, even if the data can be encrypted, access by government agencies that may require the installation of backdoors cannot be excluded.

Routing

For the sake of completeness, and for the data security aspects that will be analyzed in this Study, it is necessary to take into account the routing that currently takes place, predominantly in the United States.

25 Art. 3 GDPR.

CHAPTER 2
PROPERTY, OWNERSHIP AND OTHER DATA RIGHTS

The examination of the legal accessibility of the data presupposes that the legal relationship between the data and those who have claims on them is qualified. This relationship is a complex subject governed by a complex set of rules. Focusing the analysis for the purposes of the present Study, it is a question of establishing whether the data, as defined in the preceding chapter, can be the object of typically qualified rights (with the relative corollaries) in accordance with the legislation in force, or whether it is necessary to hypothesize new legal figures.

2.1 Data rights

Property, possession and ownership of data

From a legal point of view, one speaks of "property" when a person (the owner) has the right to enjoy and dispose of things fully and exclusively, within the limits and in compliance with the obligations established by the legal system[26].

Generally speaking, the so-called "goods"[27] that are at the owner's disposal and of which he can therefore dispose fully and indiscriminately can be the object of rights. This definition does not seem to fully cover bits, whereas it is certain and indisputable that data and information represented by them can be. To demonstrate this, it should be noted - by way of example - that such data and information can be the subject of intellectual and industrial property rights[28], whereas bits cannot be, as they are in fact a mere "vehicle" through which information and data can circulate. It is no coincidence that if a bit is deleted, it is not necessarily the case that the information or data encoded in it will disappear for that reason; on the contrary, it is reasonable to assume that they still exist, albeit encoded in another medium (whether computerized or analog).

Therefore, it is appropriate to limit the analysis for the purposes of this Study to data only, or at most to data and information, and with reference thereto to examine the potential application of the general categories of "ownership", "control" or "possession" for the purposes of the legal qualification of the various persons exercising powers and rights.

Beginning with "possession", it does not seem that the definition of the same can entirely resolve the uncertainty, since it is an excessively generic concept, only partially useful for the analysis being carried out[29]. As for "control", the legal definition of it takes us far off the subject, and does not seem appropriate to the context.[30]

With regard to the definition of "ownership", although it is not properly the object of normative codification, it is intended - according to the unanimous reconstruction of jurisprudence and doctrine, as well as the *ex adverso* reconstru ction of the many norms that refer to it - essentially the particular relationship of belonging that binds a subjective legal situation to the respective subject of law[31]. It can therefore be seen that ownership does not necessarily coincide with property and can arise regardless.

26 This is what Article 832 of the Civil Code provides, in a definition that has remained substantially unchanged since its codification.
27 In fact, according to Article 810 of the Civil Code, "goods are those things that can be the subject of rights".
28 An emblematic case, with reference to information, is for instance represented by the legal protection granted by the legal system to the so-called "Data Banks", defined by Article 2, no. 9 of Law 633/1941 as *"collections of works, data or other independent elements systematically or methodically arranged and individually accessible by electronic means or otherwise"*, and deemed worthy of protection from third parties' abuse due to their economic value.
29 Pursuant to Article 1140 of the Civil Code, *"possession is the power over a thing which is manifested in an activity corresponding to the exercise of property or of another right in rem. It may be possessed directly or by means of another person who has possession of the thing".* As can be seen, the definition may perhaps be helpful in reconstructing the "possession" of a bit by the various parties involved, but it does not help at all in defining whether those who possess such bits can or should be responsible for them upstream.
30 The term "control" is in fact the subject of many different regulatory definitions, all of which, however, are purely corporate in nature.
31 Without wishing to go into too much detail here about legal reconstructions, the etymology itself of the word leads one to consider the "title" of a right, i.e. the legally relevant act or fact, on the occurrence of which a person acquires the right (e.g.: as a general rule, pursuant to Article 2 of the Civil Code, a person acquires the capacity to act - and therefore to consciously carry out legally relevant transactions - as soon as he turns 18).

The definition would seem, therefore, to be particularly suitable to the discipline of the bit, especially if one considers that, in a field decidedly complementary to that of legal informatics, such as that of electric energy, the various regulations discipline the "ownership" of the plants that produce it in the hands of various subjects, who, in their turn, make the access and use of it "available" to others, through systems of "connection"[32]. Likewise, the use of the concept of "ownership", in relation to the content of the bits (exploiting, in this sense, also the discipline on electronic commerce[33] and that on the protection of personal data) is of undoubted help for the identification of the responsibilities and roles of the various subjects involved in the exchange, possession and control of the same.

In conclusion, for the purposes of the present analysis, it will be necessary to consider the peculiar legal relations (*rectius*: the peculiar legal relations) that exist between the owner of the data, the cloud provider and the data itself, once this is transferred within cloud systems.

Data ownership in the cloud

As we have written in the previous paragraphs, a data can be owned by a legal person as soon as the conditions that the law provides for such ownership are met. This ownership, once it has arisen, may thus translate into a right of ownership over the information contained in the data itself, but does not necessarily imply the exercise of a right of the same size over the bits constituting the data and over the infinite possible copies of the same, once the same has been digitized. This emerges even more strongly when the data, encoded in bits, is disseminated to third parties through cloud systems: consider, for instance, the dissemination of a text file online: the fact that the author of such text is the owner of it does not automatically imply that anyone who comes into possession of it through an online sharing becomes its "owner", nor - on the other hand - that the original "owner" always has the right to prohibit its dissemination. Thus, there may also be a situation in which the owner of the "information" represented by the bits is not the material owner of the bits, understood as a container, through which the information circulates (e.g. an unauthorized copy).

The beneficiary of the sharing, in turn, may at most be an abstract "possessor" of the data, until he does something legally relevant to the data, such as to configure an autonomous ownership of the same for his benefit[34].

However, the role of the technical provider who, thanks to its systems, intermediates and enables the circulation and sharing of the file and its transfer between the owner and subsequent owners, i.e. the cloud provider, is clearly different.

In this regard, it is worth recalling - a subject that will be further explored in the following paragraphs - how the cloud is a contract of a mixed nature, and for this reason it has characteristics of the traditional contract of deposit, but also of the service contract, the licensing contract and the supply contract[35]. This makes its regulation particularly complex not only (which must necessarily follow a "case by case" logic), but also and above all entails extreme difficulties in regulating a legal relationship often between subjects residing in different States (and different legal systems).

The tripartition of the types of cloud events (SaaS, IaaS and PaaS) already highlighted in §1.1, and made on the basis of their purposes and functionalities, must also be carefully considered, which adds a further level of problem, since each macro-category of contractual case presupposes different obligations and liability regimes for the service provider[36].

32 The legislative decree 115/2008 and subsequent amendments, which defines electricity grids and simple systems for the production and consumption of energy, speaks on several occasions of "ownership" of electricity production and consumption units by several legal entities.
33 First and foremost, the rules set out in Legislative Decree 70/2003 ad subsequent amendments, implementation of Directive 2000/31/EC on e-commerce.
34 This legal status is supported by the numerous Italian and international regulations on derivative works, which protect the creator of the works, without forgetting - at least on a moral level if not on a substantive level - the rights of the original works from which they derive.
35 Emblematic on this point is the wording of Art. 1677 of the Civil Code, according to which "*if the purpose of the contract is the provision of continuous or periodic services, the rules of this chapter* [editor's note: i.e. those of the contract] *and those relating to the supply contract shall be observed in so far as they are compatible*".
36 While, for instance, the SaaS cloud system provider offers software application services and will presumably have to guarantee their proper functioning, an IaaS cloud provider will, on the other hand, at least have the different obligation to make only virtualized hardware resources available to its customers.

Moreover, the cloud provider may not be the only subject involved in the data management regime, since numerous other subjects may potentially be located between it and its customer, depending on the type of data content, the nature of the cloud provider, the location of its servers and many other variables. For instance, the relationship between the cloud provider and the client/data owner could include the licensee of the particular technology thanks to which the content has been created, or - a hypothesis not as far from reality as one might think - the creator/licensee of a piece of code embedded in a content stored in the cloud. Also, the provider of a specific proprietary license for a data encryption system could come between the data owner and the cloud provider, in case of violation, modification or even termination of its license.

> *"Between the cloud provider and the customer, many other subjects may be involved in the management of the data, depending on the type of data, the nature of the cloud provider, the location of its servers, etc."*

The role of the software

Continuing on the topic of technology, the type of software used in cloud systems (mainly in SaaS systems, but not only) and the license through which this software is used also has a significant impact on the liability regimes between the data owner and the cloud system provider.

Most of the systems used for the development, management and allocation of the bits related to the data stored on the cloud are, in fact, granted under proprietary licenses; this does not mean that there are not also content management service systems and virtualization architectures in the cloud designed under so-called "open source" licenses. Depending on the type of license of the cloud management software, therefore, the management regime of the data conveyed through the same could vary and, therefore, also the responsibilities of the provider involved. We will discuss in the following paragraph how contractual provisions can and must play a decisive role.

2.2. The impact of the GDPR on civil law regulations

Data ownership between customer and cloud provider

With a view to better clarifying the concept of "ownership" of the data, what has been established so far must also be compared with the discipline of the GDPR, and the mirroring Directive (EU) 2016/680, which overlap and intersect the strictly contractual discipline to ensure the protection of personal data and regulate their use.

In fact, by virtue of the GDPR, the cloud contract is flanked, as far as the aspects strictly relative to the management of personal data are concerned, by a contract of an evidently atypical and mixed nature, the so-called Data Processing Agreement (DPA) expressly provided for by the legislation in force for the protection of personal data. This contract clarifies roles and responsibilities, in particular, with reference to the division of responsibilities between the "Owner of the treatment of personal data" and the so-called "Responsible (external) of the treatment of personal data" (a dualism which, in English, is even more suggestive, speaking, respectively, of "Data Controller" and "Data Processor"), which correspond, respectively, to the client of the cloud provider who gives the data and the cloud provider who is called to manage it.

This distinction of roles is fundamental to delineate responsibilities and obligations that the cloud provider (typically Processor) assumes towards the client (typically Controller) in relation to the processing and security of data placed in the cloud[37]. However, it should be noted that the organizational complexity of some cloud platforms, especially the largest ones, usually leads to the standardization of the provisions of the DPA, so

37 The notion of Data Processor, originally referring to persons and entities that process personal data on behalf of the Controller and that may or may not also be present within the Controller's organization itself, has been modified following Opinion 1/2010 - WP 169 of the Art. 29 Working Party on the concepts of *"controller"* and *"processor"* (https://www.garanteprivacy.it/documents/10160/10704/wp169+-+Opinion+1+2010+on+the+concepts+of+ controller+and+incumbent+processors.pdf/64cd4700-f0d4-4c04-b834-9-c3da69a93ea?version=1.1), the concepts of which were then transposed into the GDPR. To date, the notion of Data Processor, defined in Art. 4(1)(8) of the GDPR as *"the natural or legal person, public authority, service or other body that processes personal data on behalf of the controller"*, expressly regulates - together with Art. 28 GDPR - the role of a subject exclusively external to the controller's organization.

that the owner is called upon to give his newly appointed "controller" an assignment based on standard prescriptions decided by the latter, and normally not very negotiable, tailored on the data management services that are activated.

However, the scope of the GDPR is certainly not limited to the requirement for a DPA.

Right from its definitions, the GDPR contributes to outlining some phenomena of crucial importance, not only as regards the type of data that can be shared and exchanged, but also in the very qualification of the activities that can be carried out, with specific reference to that particular type of data[38].

As already pointed out in §1.2. above, the very definition of "personal data" codified in Art. 4, N° 1) of the GDPR, exponentially expands the operative dimension of the protection of the personal data, going, for the first time in the European ambit, to include *"any information regarding an identified or identifiable natural person".* It is easy to see that this is a broad definition, almost disproportionate with respect to the scope of the regulation, which cannot but be taken into account also outside the scope of the same. The definition of the activities of "processing" in n.2) of the same Article 4 completes the circle, covering *"any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".* These definitions require careful consideration of any activity carried out with regard to potentially personal data, locally or in the cloud, precisely because such activities are themselves potentially covered by the concept of "processing".

The GDPR, in fact, consequently, provides for a series of obligations and rights for the Data Controller, who determines the modalities and purposes of such activities with regard to the data, different from those due to the Data Processor, who, in turn, carries out data processing activities on the express mandate of the Data Controller, and indeed complies with the instructions that the latter provides[39]. This is, on closer inspection, the conferral of the widest range of powers on the Data Controller, and this actually seems to be in open contrast with the contractual discipline of the cloud, where it is actually the Data Processor, i.e. the cloud provider who "lays down the law" on the conditions under which he stores the files on behalf of the Data Controller. In fact, it is the cloud provider who decides the conditions under which the customer can use the various services purchased, and the customer - except in rare cases - has no choice but to comply with them, often accepting more than one DPA in this regard[40].

The paradoxical consequence is that at the contractual level, and in particular in the terms and conditions of the cloud services, a Data Protection set-up is established on the basis of which the customer, who assumes himself to be the Data Controller, often appoints the chosen cloud provider as his external data processor, for the activities falling under his responsibility, limited in relation to the relevant Service Level Agreements (SLAs).

What is certain and common to the two (evidently different, although similar) situations, is however that only the Data Controller is by law the only subject who can perform all the operations on the data that are proper to his role; and that he is actually the only one responsible, in terms of content, delegating to the cloud provider (his Processor) a more limited corpus of powers concerning the data entrusted to him, specifically functional to the type of service subscribed.

38 It should be pointed out at the outset that, although the GDPR expressly refers to specific types of data (which will be discussed shortly), it provides a general framework appropriate for use for a much wider range of generic "data".
39 This arrangement, provided for by the interaction between Articles 24 and 28 of the GDPR, is actually outlined by the same definitions of the two subjects, nn.7) and 8) of Art. 3 GDPR, and is codified as "accountability"; it translates into a greater burden of responsibility on the Owner, who determines means and methods of processing at his full risk and responsibility), but who can then pour specific responsibilities on the external manager to whom he entrusts the data, and on whom he can then rely on a contractual level, in case of non-compliance.
40 Pursuant to Article 28(3) of the GDPR, *"processing operations by a controller shall be governed by a contract or other legal act in accordance with Union or Member State law, binding the controller to the data controller and stipulating the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and the rights of the controller."* This specific act, the specific contents of which are further regulated in the continuation of the paragraph in question, often takes the form of a Data Processing Agreement, often in conjunction with the clauses and provisions required for non-EU processing, in accordance with Articles 44-49 of the GDPR on the subject.

The problem of transferring data abroad

Among the fundamental provisions of the GDPR, as is well known, is the prohibition[41] to transfer personal data outside the European Union in the absence of an adequacy decision by the Commission certifying that the country or international organization to which the transfer is made ensures an adequate level of protection for the personal data in question.

In the absence of the aforementioned adequacy decision, the Regulation only allows the data controller or data processor to make the transfer in the presence of "adequate safeguards", which are exhaustively provided for[42] and among which, for the purposes of the present discussion, the so-called "standard contractual clauses" adopted by the European Commission, the "binding corporate rules" and, secondarily, the contractual clauses between the data controller or the data processor and their counterparts (or the recipient) in the third country where the data are to be transferred are of particular importance.

As of 16 July 2020, with respect to transfers to the US, only the second tier of tools can be used to make cloud (and non-cloud) transfers of personal data, as in a disruptive judgment (the so-called "Schrems II" decision), the EU Court of Justice invalidated the so-called "Privacy Shield" adequacy agreement that had been regulating and permitting personal data transfers between the EU and the US since 2016, allowing data to be transferred under a regime similar to that of the GDPR, thus without any special formalities.

The practical result is that, from July 2020 onwards, any transfer of personal data to the US, in order to be lawfully made, must be assisted by one of the additional safeguards set out in the GDPR, which in addition, may be subject to further specification by the European Data Protection Board (EPDB).

Additional limitations imposed by the GDPR

Another issue not to be overlooked, again with specific reference to the legislation on the protection of personal data, is that of the effective legal limitation of the "automated" and "by design" uses of personal data: as is well known, pursuant to Article 25 of the GDPR, all entities processing personal data must ensure that their processing systems are, from their design, structured to process only the personal data that are genuinely necessary in relation to the service (so-called "minimization" or "privacy by design") and, pursuant to art. 5 GDPR, process data by default in a secure manner that respects privacy rights (so-called "privacy by default"). In addition to these obligations, it is objectively impossible for any Data Controller or Data Processor to carry out processing operations based exclusively on automated logic (first and foremost, that which leads to the profiling of data subjects on the basis of specific information relating to them), without the express consent of the data subject or specific legal provisions, as referred to in Article 22 GDPR[43]. The operating margins of the cloud provider to whom the data are entrusted by the Data Controller therefore encounter further restrictions on access and use, which must be taken into account when examining the liability regime.

It must be said that these limitations are not absolute since the GDPR:

- concerns only personal data, and therefore non-personal data, including corporate data (see above, § 1.2.), remain outside its scope;
- allows EU Member States to introduce restrictions where deemed necessary to reconcile the protection of personal data with the freedom of information and expression (Art. 85) or for reasons relating to archiving requirements (Art. 89).
- It also allows limitations on its effectiveness and application for reasons of national security, defense, public security and the prevention, investigation, detection and prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security (Art. 23), provided they are necessary and proportionate in a democratic society and respect the essence of fundamental rights and freedoms.
- In addition to these specific provisions, Article 2§2 excludes entirely from the scope of application the

41 The prohibition in question is derived from Article 45 of the GDPR.
42 See Article 46(2) and (3) GDPR.
43 The provision is specifically designed to protect the right of data subjects to ensure that their personal data are not subjected to processing that is particularly "invasive" of their personal sphere, as it is likely to have a significant impact on it.

subjects of border control, asylum, immigration and police and judicial co-operation on criminal investigations.

It should also be noted that, on the other hand, as regards the processing of personal data in the field of crime prevention, investigations, enquiries and criminal proceedings, it is regulated not by the GDPR, but by Directive 2016/680, transposed in Italy by Legislative Decree 51/2018. However, the different approach between the two regulations leaves some margins of intervention to the States: the GDPR does not apply to cases of national security, and neither does Directive 2016/680 (unless there are investigations into crimes or needs to prevent security threats).

In conclusion, EU Member States retain some leeway to take action on personal data when there are national security needs, regardless of a concrete threat. In such a case, the GDPR does not offer protection to personal data. Obviously, the general EU principles of transparency of administrative action and the right to be heard remain in force and, therefore, any transfer and use of data could not take place without notification to the data subject, but consent may not be a necessary element for there to be access or transfer of personal data in such cases.

CHAPTER 3
THE LEGAL FRAMEWORK GOVERNING DATA REACHABILITY IN THE CLOUD

3.1. The cloud contract and the relevance of the contract type

Having established in the previous chapter the relationship between data and their holders, in the light of both civil law and the GDPR, it is now necessary to analyze how this legal relationship is expressed in the context of contracts governing the "cloud" relationship.

The general issue: limits and effects of the "negotiability" of the cloud contract

The contract with which cloud services are purchased and provided is a fundamental and crucial aspect for the issue of legal reachability of data. In fact, depending on the type of contract drawn up, it is possible - in the various cases that arise - to deal with different availability/accessibility structures of the data between the customer (i.e. the original owner of the data) and the cloud provider who, depending on the service rendered, may (or may not), as mentioned above, also become an owner of the data, or merely process them according to the instructions received, sometimes in encrypted and inaccessible form.

This is a delicate analysis because, as mentioned above, the type of contract regulating the relationship is mainly chosen by the cloud service provider, while the customer's ability to negotiate is often limited (at least for the type of contract, whereas greater autonomy may be exercised for certain economic and technical conditions). Moreover, the different legal systems in which the various cloud providers active in Europe operate (some even in more than one jurisdiction) may provide for different rules for the various contract types.

The picture is further complicated by the fact that international law makes it possible to determine by agreement the contractual law applicable to the contract, so that an act entered into in Italy may be subject, by the will of the parties expressed in the contract, to the law of a third State (e.g., according to the most common cases, to the laws of the United Kingdom or Northern Ireland, or even of US States such as New York, New Delaware or California). In the majority of cases, these laws are completely different from the Italian law and, except in rare cases, are not known to the foreign parties who have to accept them.

The parties could also establish (or, rather, have to accept) an ad hoc jurisdiction for any disputes, with the result that any legal action against the cloud provider would have to be judged by a non-European court (in the USA, for instance) or by international arbitration, with costs and burdens that could be very different from those the party would bear for a similar domestic dispute.

However, even in cases where the contract is governed by Italian law and the forum for litigation remains in Italy, it can be observed that the cloud issue, and in particular the related contractual configurations, is not yet consolidated in many Italian courts. Jurisprudence (which is permanently delayed due to the historical backlog of judicial offices) has so far dealt mostly with issues relating to software projects to be carried out on site, while there are no recent rulings at national level that clarify the fundamental aspects of the relationships within the cloud contract for which, therefore, we rely mainly on the development of legal doctrine.

Contractual regulation and impact on data reachability

Compared to an initial flourishing of rather general "cloud" contracts that did not describe the characteristic aspects of the service, the need for specificity in this type of contract was soon realized.

It is in fact particularly important that the contract for cloud services clarifies the fundamental aspects of the relationship between cloud provider and customer/data owner, and is also particularly explicit as regards its qualification. Only in this way will it be possible to easily determine the rules applicable to the case, especially in relation to the entrusting of data to a third party who, according to the contractual provisions, does not become the owner or, rather, should not normally become the owner unless there are specific needs that are justified in the contract.

In fact, from the moment that the data start to be outsourced to the third party and no longer reside on the client's local infrastructure, and even though the user has only a minimal perception that the data have been stored on a remote server, from a legal point of view a fundamental transformation of the relationship between data controller and data takes place that can be summarized as follows:

- availability and accessibility of data in the hands of the customer/owner continue to exist, but only insofar as the third party, i.e. the cloud provider, provides the service in the forms governed and regulated by the contract;
- the customer/owner has the data not because he/she accesses something in his/her possession, but rather because he/she benefits - twenty-four hours a day - from a service provided by the cloud provider who, however, could at some point find him/herself in the position of not fulfilling the contract, either intentionally or due to force majeure (with consequences, even serious ones, on the availability of the data for his/her customer)[44].

Therefore, the contract plays a fundamental role, especially in the presence of critical and unforeseen factors: if it is not sufficiently clear, detailed and appropriate with regard to the type of needs and protection required by the specific contracting party (e.g. a hospital, a law firm, an insurance company, etc.), any detrimental event for the parties, including disputes and misunderstandings, could cause devastating consequences, with prolonged inaccessibility of data or even loss of data.

It is also important that the contract regulates the measures that the cloud provider will adopt in relation to the type of data to be managed (sensitive, personal, business secrets, etc.) and that the customer, before doing so, correctly informs the cloud provider of what these types of data are and the expected level of security. In fact, not all data require the same security measures and have the same discipline with regard to the times and methods of storage and, when the data are managed by a third party (the cloud provider), the latter will have to ensure compliance with the resulting legal obligations.

To sum up, the cloud contract constitutes the fundamental legal instrument that regulates the provision of the cloud service in all its aspects. It determines the specific nature of the service provided by the cloud provider, the regime of the operator's responsibility for the entrusted data and then, ultimately, the issue of reachability.

A few examples may better clarify the critical issues that may arise in the case of imprecisely drafted or poorly detailed contracts:

- on a technical level:
  - switching from one cloud provider to another could lead to difficulties in getting data exported in a standard format;
  - the customer may have to restore large amounts of data from the cloud without having agreed with the cloud provider on a clear timeframe for recovery (in the absence of adequate SLAs);
- on a contractual level:
  - the terms of the contract may not have defined the obligations of the cloud provider with regard to the return/deletion of data, which, instead, should be precisely defined in every cloud contract;
  - events such as the bankruptcy of the customer[45] (with consequences on payments), insolvency proceedings, and even simple non-payment/late payment of services could result in the cloud provider refusing to grant access to the data;
  - where the cloud contract provides for the processing of data outside the EU, it must be contractually ensured, by means of EU-approved "standard contractual clauses"[46] (usually incorporated in an annexed DPA), that the cloud provider will comply with the relevant provisions of the GDPR, e.g. by ensuring adequate data security and promptly notifying the data controller in the event of a data breach;

44 See for example https://www.corrierecomunicazioni.it/digital-economy/blackout-mondiale-per-google-services-tutto-risolto-in-poche-ore/; https://st.ilsole24ore.com/art/tecnologie/2011-04-29/incendio-server-arubait-tilt-121947.shtml?refresh_ce=1; https://www.bbc.com/news/technology-36460328.
45 See https://www.hostingtalk.it/cloud-computing-quando-il-provider-fallisce_-c0000067g/.
46 See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

- certain types of data controllers (e.g. banks and financial institutions) are subject to specific regulatory obligations regarding the management of data in the cloud, including the right of the data controller to periodically audit the cloud provider, and the requirement that any third-party access requests to the data be promptly notified[47] ;
- in the case of subcontracting (where not prohibited by the contract), the guarantees provided by the cloud provider must be the same that the cloud provider will impose on third party subcontractors, and their territorial scope should be disclosed and authorized in advance by the customer. Indeed, if the customer commissions services from a cloud provider on the basis of specific guarantees and territorial scopes on how and where to store the data, it must be ensured that the operator does not circumvent these agreements by entrusting the data to third parties (and thus determining the possibility of further "reachability" of the data by third States).

The aforementioned issues obviously have a fundamental impact on the general "reachability" of the data entrusted in the cloud and, therefore, can (and should) find definition in the context of a well-structured contract. In what follows, however, it will be observed that standard contractual arrangements often do not allow negotiating the ad hoc content of a cloud contract, but that, at the same time, there are "imperative" reachabilities that cannot be contractually excluded. The consequence of this may even be that the choice of contract will be made by changing (or choosing upstream) the cloud provider that presents the best compromise from a contractual point of view. Therefore, in assessing possible criticalities arising from the data reachability, a careful custody of data in the cloud must strike a balance:

- factors that can be managed by contract, since they depend on the type of contract signed between the data owner and the cloud provider, obviously taking into account the law applicable to the contract itself;
- the jurisdiction in which the cloud provider itself and its subcontractors operate, as well as that of the place where they intend to host the data that will be managed and processed in the course of the contractual activities.

We shall now see what are the specific features of the cloud contract in the Italian legal system, generally valid in all European legal systems of the same matrix, but decidedly different in Anglo-Saxon systems such as the UK and the US.

3.2. The cloud contract in Italian law

The cloud contract as an atypical contract

The cloud contract for the law is what is known as an "atypical" contract, in the sense that in Italy there is no rule regulating the specific "cloud" contract. However, it does not follow that the type of obligations contained therein are unknown to the law. In fact, the contract for cloud services, regardless of its express qualification as such, can in fact be traced back to certain types already regulated by the Civil Code and contract law and, above all, not unknown to the law.

This operation is particularly important already during the negotiation/conclusion of the contract, since the more a cloud contract contains at its origin the characteristics of the so-called "typical" contracts, the more the eventual criticalities that may arise will be solvable according to consolidated and easily traceable criteria and legal interpretations. Similarly, it will be possible to more clearly identify the division of responsibilities related to data storage and processing between the customer and the cloud provider, as well as the situations in which the cloud provider is required to give access to data to the competent authorities.

In short, it must be borne in mind that the cloud contract presents aspects of considerable complexity that require the more important the outsourced data (corporate or personal), the more careful advance planning is required, since, in the event of a critical situation, an unclear contract makes it difficult to provide protection

47 See for example the EBA Guidelines on outsourcing to cloud providers, which are binding for the financial and insurance industry: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers.

after the event.

Only as far as the SaaS cloud contract is concerned, in fact, there are at least three different orientations[48] that lead it back, respectively, to the contract of service contracting, to that of service administration or to the outsourcing contract. On the other hand, for IaaS and PaaS, among the prevailing orientations, it is noteworthy that one which leads them back to the discipline of the rental contract (with the consequent responsibility of the provider for the good functioning of the hardware and the placement of the same in suitable premises, together with the other obligations of preparation and programming of the service itself for the purposes of the user's interest and the provision of the assistance service): this approach has the benefit of keeping the means for the provision of the service (hardware and basic software) in the hands of the provider, leaving instead entirely in the hands of the user all responsibility for the contents stored through the service[49] .

However, cloud contracts can never be pure leases, but are always a hybrid of lease and service contract. This becomes evident when one considers the disclaimers traditionally attached to cloud contracts, which in a traditional lease would be virtually null and void under the ordinary rules on defects of the leased thing and the conventional limitations of the lessor's liability[50] . Another doctrine prefers instead to trace the specific discipline of the IaaS cloud services - always in the form of mixed contracts with the contracting of services - to the traditional deposit contract, placing at the charge of the provider the typical obligations of a depositary[51] : the cloud contract would thus be a hybrid between the regular case of the deposit (for which a depositor entrusts the depositary with a "good" to be kept without using it for personal purposes and to be returned at the end of the deposit) and the so-called "irregular" one (i.e. a depositor deposits a certain quantity of goods, which the depositor can use, being however obliged to return, at the end of the deposit, the same quantity of the type of goods deposited, e.g. food, energy or, in this case, "data").

Essentially, irrespective of the reconstructions and the cases recalled, in a well-structured cloud contract one can identify, as a "typical" element, the relationship for which the ownership and the full exercise of the rights on the data lie with the actual user, while for the cloud provider a series of obligations are configured, more or less extensive according to the type of cloud and infrastructure, correlated to the storage of the data in question. In particular, contracts must define a set of rules that establish the standards that the cloud provider will apply for data storage and security, as well as service levels and obligations for the management of emergency and contractual events (e.g. what to do with the data at the end of the contract). Similarly, the contract should establish responsibilities for damage and inaccessibility of data, e.g. in case of force majeure events.

Specific contractual provisions shall also be devoted to the behavior of the cloud provider in the face of requests coming from "competent" authorities and according to the "applicable" law. It is to be hoped that, the greater the relevance of the data stored/processed in the cloud infrastructure, the more detailed these provisions will be, to the point of referring to actual procedural documents describing the policies applied to the requests received by the cloud provider, with examples of the same[52] . In fact, as we shall see below, there may be cases in which, by virtue of the data processing services provided, the cloud provider may find itself managing data in the capacity of actual owner, having full possession of them.

48 The plurality of orientations also derives from the different possible contents of the SaaS cloud contract: the data processing entrusted to the cloud software may in fact have different purposes and different contractual relevance, thus changing the applicable contractual type and the responsibility of the cloud provider. One thing is the monthly processing of salaries or the keeping of company accounts, another is the cloud-based use of an online video game.

49 Pursuant to Art. 1575 of the Civil Code, the landlord has three fundamental obligations: *"1) to deliver the leased property in a good state of repair; 2) to keep the property in a state to serve the agreed use; 3) to guarantee to the tenant, during the tenancy, the peaceful enjoyment of the property".* To these obligations must be added those set out in articles 1576-1577 concerning the maintenance of the leased property and its repairs, which assign to the landlord the activities of extraordinary administration, leaving to the tenant the ordinary ones.

50 Articles 1578-1581 of the Civil Code, according to which the landlord is liable for defects in the leased property (whether existing or occurring) and must compensate the tenant if he does not prove that he was unaware of such defects without fault at the time of delivery.

51 First, the obligation to receive the goods (the data) and to keep them with the diligence of a good father, according to the provisions of Articles 1766 et seq. of the Civil Code.

52 Interesting in this respect is Google's "Transparency Report" available at URL https://transparencyreport.google.com/?hl=it and dealing with "Sharing of data that reveal how government and company regulations and actions affect data privacy and security, as well as access to data": within this report, at URL https://transparencyreport.google.com/user-data/overview?hl=it there is a special section listing data on global user information requests received by Google. In particular, with regard to Italy, we read that in the period July 2019-December 2019, out of 1486 requests relating to 2099 accounts, Google fulfilled, in whole or in part, about 50 per cent of them.

The most relevant types of civil law: administration and service contracting

The legal doctrine, following the analyses mentioned above, now considers that the type of contract that best represents the obligations that characterize the cloud contract is the so-called "service supply contract", known in most European civil law systems as *"service provisioning"*.

Article 1559 of the Civil Code defines "supply" as a contract by which one party undertakes, in return for a price, to perform, for the benefit of the other, periodic or continuous services of things. In the case of the cloud, the obligation obviously concerns the provision of services.

This is a contract other than a procurement contract because the services are standard and not made to order, they do not have to be "tested" in order to be supplied, and the supply takes place according to precise time frames, against which the right to periodic payment accrues. The service is thus rendered for an indefinite period of time or in any event over an extended period of time, whereas a contract is normally used for a contingent need and does not provide for continuous payment.

The contract will thus be governed by the rules of the Civil Code on supply contracts, whereas the rules on service contracts may be applied to the present case only in the alternative and in so far as they do not conflict with the rules on supply.

The "genetic" difference between service contracting and service delivery with regard to the cloud, which makes it possible to understand immediately which is the contractual type to which the contract refers, can be identified with regard to the provisions of Art. 1560 of the Civil Code. In fact, this provision allows the supplier providing the supply to enter into the contract without exactly determining the exact amount of the supply that will be required by the customer during the contractual period, it being possible to determine only the maximum and the minimum since, for the rest, it is *"intended as agreed that which corresponds to the normal needs of the party entitled to it"*; which is instead problematic in the contract of supply, where a design specification of the supply that the contractor is provided by the contractor is required.

In the contract of supply, moreover, payment of the price is determined, according to Art. 1561 of the Civil Code, having regard to the time of expiry of the individual services and the place where they are to be performed. Thus, the price stipulated for each term is not repeatable in the event of termination, since the service is complete and in the event of a dispute as to the performance of the contract the customer may not claim the months preceding the first dispute and already paid.

Moreover, the prohibition of subcontracting under Article 1656 of the Civil Code was held not to be applicable to the contract qualified as supply. However, this is based on the assumption that the services supplied (in our case in the cloud) are not the subject of *ad hoc* design (e.g., created for the needs of a specific customer) but are attributable to the standard services of the cloud provider. This implies that a cloud provider could legitimately use - subject only to the obligations deriving from the GDPR in terms of appointment of data controllers and related disclosures - other subjects as subcontractors of components of the supplied service and, as mentioned, such subjects could operate in different territories and, even, on the basis of a different applicable law.

Choice of contract type and consequences for data ownership and reachability

The contractual configuration described above leads us to outline a legal framework in which the data is entrusted to the cloud provider, but without the latter acquiring any ownership over it; unless a data processing service is requested from the provider, which entails its management "in a clear manner" and requires the knowledge of the data by the operator.

The cloud provider, in fact, does not "buy" the ownership of the data, but provides a service to support the integrity and security of the data themselves and, in the sole case of SaaS, performs a data processing service which, however, always remains the property of the customer. This is comparable to the case of parking in a garage: the garage owner can start and move the car only as far as necessary to park it, but does not acquire ownership of it, nor can he carry out any intervention on it. In other words, he does not have full possession of it, and the possibility of using the car is only for custody purposes, so that if he were to "take a drive" with

the car in custody, he would be committing the offense of embezzlement.

As already mentioned, a part of the doctrine sees in the entrusting of data to the cloud provider similarities and elements compatible with the custody and with the same contract of "deposit", so that one could find in the cloud contract thus configured a mixture of obligations of the supply combined with those of the deposit (rather than with those of the service contract). Using this regulatory scheme[53] to anchor this case to well-established rules of the Civil Code and related case law, the obligations of the cloud provider are clear: having obtained the data from the customer, he can only use them in the manner specified by the customer and, as soon as requested, he must return them (e.g. by allowing the reading and downloading of the file) or even delete them (in case of final return). According to this reconstruction, the cloud provider therefore has no availability of the data for its own purposes.

These elements are of particular importance for the purposes of this Study, as they allow to establish who is entitled to the actual ownership, availability and accessibility of the data - even during the contract and even while the data are on the cloud provider's servers. As a matter of fact, in the presence of a properly structured cloud contract, the data is located where its owner is and, if the cloud provider does not own it (as defined above), it cannot be at the same time at the cloud provider.

Therefore, any measure concerning data stored at the cloud provider (which does not have the ownership of the data) but not directed to the data owner would be potentially unlawful: the cloud provider would not be able to hand over to third parties a data of which it has no availability, just as a bailiff cannot seize a leased asset when it is pointed out to him that the owner is not the company owner but the finance company.

However, in cloud contracts of the PaaS/SaaS type, what has been said so far must be reconciled with the fact that the object of the contract does not fall within the types of cloud directly referable to the custody of the data: the data is in fact necessarily provided to the cloud provider in order to obtain its processing and transformation into a "different" data through the platform and/or the software present on the systems of the cloud provider. The above contractual types - which are also applicable regardless of their express reference and on the basis of the ex post analysis and interpretation of the contract - are thus associated with different degrees of obligations and responsibilities for the custody and management of the data and, in these cases, as already suggested above, the remedy consists in agreeing with the cloud provider on the procedures that the same must follow in the face of requests for access and regulate, on the basis of such information, the types of data that can be outsourced.

On the contrary, on the basis of the preceding statements, it is possible to affirm that in the case of the IaaS, the cloud provider, in the presence of an adequate contractual configuration that incorporates the elements suggested above, normally does not have possession of the data that it treats: in these cases, the contractual element is also accompanied by the technical element (diriment) for which the data are encrypted with a key inaccessible to the cloud provider to sanction a barrier between the data (of the client) and the service (of the cloud provider)[54] as evidence of this lack of possession and availability, just as the goods deposited in a safe deposit box are not accessible for the bank that hosts the same box.

It goes without saying that it is not always possible to obtain a cloud contract subject to Italian law (or another European state with the same civil law matrix), nor can such a contract always be negotiated to obtain the type of contractual structure that best suits one's interests. Therefore, it is also necessary to assess scenarios unrelated to local experiences, such as those of an atypical cloud contract governed by a foreign law of a different matrix: US law, Chinese law, Korean law, etc... In these cases, the assessment of the contract must be carried out by analyzing its obligations and reconstructing what the cloud provider guarantees with respect to the data that the customer entrusts to its management.

It must also be examined whether or not the cloud provider allows the customer to decide on the geographic location of the servers that will process the data in the cloud, since this geographic location, determined in the contract, is of specific relevance - as will be noted in Chapter 4 - for the operation of specific provisions

53 The best way would be to declare expressly applicable (in a contract subject to Italian law) both the rules of Art. 1560 et seq. of the Civil Code and, for all other aspects, the rules of Art. 1766 et seq. of the Civil Code.
54 Regardless of the "strength" and inviolability of the encryption. The fact that they are encrypted constitutes a logical barrier, like a door that is locked but which could be broken down with a light push: the fact that the door has to be "broken down" forces the cloud provider to take illegal action, which makes any obtaining of the data illegal.

that allow certain jurisdictional and governmental authorities to order the cloud provider to produce the customer's data.

The particular regime of data processed in SaaS cloud services

As already highlighted, in the SaaS cloud contract, the cloud provider's performance takes on a particular connotation. Indeed, it does not merely provide a space where the customer can store data. The cloud provider takes delivery of data that it processes using its own software tools on its own platforms, returning the result of the processing to the customer in the form of service.

It cannot be said that the cloud provider's performance is limited to the remote supply of software because this software never enters the customer's possession: the cloud provider provides "access" licenses to software installed on its own infrastructure.

The data resulting from the processing carried out by the cloud provider from the data transmitted by the customer by virtue of the SaaS service (e.g. even only returning a pdf file against the input of simple text or returning a retouched photo against the input of the original) are thus to be considered as data generated by the cloud provider, and therefore falling within its sphere of ownership, at least until the moment of the "delivery" to the customer. Even after this delivery, however, the contract may provide that the cloud provider retains certain rights over these data (e.g. intellectual property rights over the form in which they have been processed, e.g. the graphic form of a presentation).

Furthermore, it is possible, according to some theories, that to the systems in cloud and of big data, the regulations for the protection of the databases are applied (the so-called sui generis right provided in the EU by the Directive 96/9/EC) for which, in the moment in which the client of the cloud provider "feeds" the cloud system with data, it is inserted in a structure that - as fruit of the investments of the cloud provider - is of ownership of the cloud provider. Consequently, the extraction (i.e. the subsequent retrieval of the data using the database) becomes a right that the cloud provider "grants" to its customer on the basis of the contractual agreement, without prejudice to the customer's ownership of the raw data.

Otherwise said, in the face of a greater complexity of the cloud services that are rendered, especially in a SaaS regime, and in the absence of a clear contractual provision whereby the cloud provider does not retain any ownership of the managed data, it is highly possible that an external authority identifies the cloud provider, and not the customer, as the one having ownership or possession of the data, or part of them, in the moments of the service just after their processing in plain text in the cloud systems.

In view of this, in the face of legal provisions providing for the accessibility/reachability of data in the availability of the cloud provider, a contract not sufficiently precise in this respect would create uncertainties and criticalities that could open the way to requests for data access made by foreign authorities to cloud providers subject to their jurisdiction, as will be further discussed in Chapter 4.

However, it must be said that, at contractual level, the enforcement of such foreign rules might find a greater difficulty in contracts where the applicable law and the jurisdiction agreed upon by the contracting parties were nevertheless maintained within the European Union since these parties, even if they had to counter access requests of foreign governments, would still have to discuss them before a European court and on the basis of a law of an EU State.

3.3. Data not in conformity with contractual agreements

The analysis carried out so far has aimed at defining the legal status of the data, identifying its owner and the ideal contractual context, in order to assess the basic conditions for legal reachability.

However, consideration must also be given to the hypothesis that the data are held by the cloud provider in a different context, namely non-compliance with legal or contractual rules.

The question is whether the (in principle unwanted) presence of data not in accordance with contractual agreements or in breach of the law on the cloud provider's systems changes the legal "title" to hold such data,

requiring the cloud provider to treat them differently from data lawfully held on the basis of contract or law.

To this end, the contractual prohibitions imposed by the operator on the customer as a result of the so-called Acceptable Use Policy (AUP), i.e. the contractual annex in which the permitted uses of the hardware and software infrastructure offered by the cloud provider are regulated, are of specific relevance.

In fact, if the customer breaches the AUP (which is often unknown to the customer, being a contractual document signed upstream by the contractual referent), the breached data would not be "compliant" with the contract and as such, could not be managed by the cloud provider, having, in theory, to be "returned" to the customer.[55]

The following question therefore arises: could data that is not compliant with the AUP, and therefore (potentially) not subject to its custody, be considered "reachable" by possible measures of public authorities? For instance, it could be a case of files containing health data or copyright infringing content where the AUP would prohibit the storage of such kind of data in the cloud infrastructure.

In principle, reasoning with the principles regulating the liability of the hosting provider contained in the Directive 2000/31/EC on e-commerce, applicable also to the cloud, until the non-compliant data were not validly reported to the cloud provider (and/or returned and deleted), the cloud provider would not have a legal "awareness" of it and would have to manage it in good faith like any other data. Therefore, the regulation of the reachability of this data would not be so different, at least until the data is "reported". At that point, the non-compliant data would be, so to speak, an anomalous object, no longer covered by the contractual provisions and entrusted to the cloud provider only de facto: it would be the cloud provider who would still have possession of it in the phase in which it is not yet returned or destroyed, and it is believed that, as a consequence, this would expose the data to reachability to a greater extent than data that are instead compliant with the contract.

Also, a contractual discipline that would allow the cloud provider to carry out preventive or random checks, for example, because of copyright protection, should be carefully parameterized: non-compliant data should not be forfeited in order not to create an anomalous corpus in the management of cloud data, potentially attackable by measures of any kind and difficult to eliminate without the involvement of the user.[56] Such checks could be contractually convenient for the cloud provider to avoid that the authorities could hypothesize a co-responsibility of the provider itself, in the face of massive uploads of illegal contents[57].

The AUP and the contract constitute the first reference for the relations between the user and the cloud provider, especially in situations where the cloud provider is ordered by a competent authority to inhibit the service to a certain customer or regarding certain data. In fact, even if the order is issued by the competent authority, the cloud provider, by executing it, thus potentially defaults towards its customer, unless the contract does not provide for liability exclusions with regard to such a situation or there is a clear situation of default on the part of the customer - for instance because, as in the examples above, it has transferred to the cloud provider types of data not allowed by the AUP. In situations of uncertainty, the cloud provider might be forced to keep data seized by the authority while waiting for measures to be taken in this respect, without being able to finally get rid of it, in order to protect any rights of its customer.

55 A recent case that has caused a lot of uproar is the Amazon-AWS/Parler case, in which the American cloud provider interrupted the IaaS service of Parler, the favorite social platform of the American right-wing Trump supporters, effectively shutting it down. According to Amazon-AWS, Parler had violated the AUP due to false or dangerous content disseminated by users, thus necessitating the measure. Parler filed a lawsuit against Amazon-AWS (see: https://www.bbc.com/news/technology-55615214) on the grounds that he did not violate the AUP.

56 In the US Department of Justice's case against the *cyberlocker* Megaupload, which alleged the primary use of the service for sharing *copyright* infringing content, the service was shut down and the servers seized. Nonetheless, the question of whether (and how) data could be deleted, the storage cost of which was estimated at USD 9,000 per day, was a complex one. In fact, a theoretical interest of the users in recovering the data was recognized, even though the terms of use of the service warned users that storage entailed the risk of complete loss of the data at any time. Finally, the data were placed under the protection of the EFF (Electronic Frontiers Foundation) as a neutral body in charge of handling the remaining requests from users, to be carried out within a maximum time limit.

57 Such liability was alleged in the above-mentioned US case of the cyberlocker Megaupload on the basis that the cloud service in question had been designed and marketed for primary use in violation of the law. The case, however, never reached a substantive discussion, as termination of the service and criminal prosecutions took place before that. In the EU, the new Copyright Directive 2019/790 excludes "business-to-business cloud services" and "cloud services that allow users to upload content for personal use" from the special liability for content uploaded by users that it outlines: it ascribes the new liability regime to entities defined as "providers of online content sharing services", namely those whose main purpose or one of the main purposes is to store and give access to the public to large amounts of copyrighted works or other protected material uploaded by its users, which the service organizes and promotes for profit.

Finally, it should be noted that the analysis of the subject matter identifies regulatory or quasi-regulatory measures that establish a reachability "regardless" of the contractual structure.

Such are, for instance, the provisions regulating the availability of cloud data of investigated subjects during the inspection activities of independent authorities. These provisions establish an equivalence between the reachability of the data in the cloud and the accessibility of the same in an attempt to provide legal cover to copy/seizure operations carried out during investigations of independent authorities (e.g. antitrust) of any data that is accessible in the cloud to the investigated person, omitting to verify whether or not there is contractual ownership of the data or intellectual property of the same in the hands of one or the other, and without having to give up the apprehension where the data has been outsourced.

This describes a, as it were, "functional" accessibility, which allows the proceeding authority to acquire the data in a broad manner, justified by the purpose of use limited to the proceedings in progress and by the regime of its investigative secrecy (without prejudice to the possible future right of access in omitted form of the third parties concerned).

This is a case of access to which the European Commission's Competition DG, among others, has often resorted (since 2013[58]). However, this procedural width has found in recent years a lively opposition based on Article 19 paragraph 2 of the Budapest Convention of 2001[59] on the fight against cybercrime (where the powers of the antitrust authorities are equated to the criminal judiciary in the inspection). This provision provides that *"Each Party shall take such legislative and other measures as may be necessary to permit that, where its authorities search or similarly access specific computer systems or parts thereof in accordance with paragraph 1.a, and have reason to believe that the data sought are located on another computer system or part thereof in its territory, and access to such data is lawfully possible from the initial system, the same authorities may expeditiously extend the search or access to the other system"*.

Consequently, the apprehension of data on foreign servers, on the basis of the possibility of access, as provided for by the Budapest Convention, in hypotheses of computer crime or similar, appears to be possible only where there are specific agreements between the two States (such as those provided for by the US CLOUD Act, which will be discussed in Chapter 4 below).

58 See Commission Explanatory Note https://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf
59 See https://rm.coe.int/16802f423d.

CHAPTER 4
PUBLIC AUTHORITIES' INTERVENTION IN DATA REACHABILITY

As highlighted in the previous chapters, the legal configuration of the cloud, as per the legislation applicable territorially and by virtue of the chosen contract, has a significant impact on the reachability of the data for the purposes of extracting the information. This has important repercussions on the accessibility of the data and on the *modus operandi* to be followed by the proceeding authorities (e.g. the judicial authorities in search of digital evidence or illicit material) with purposes, alternatively, acquisitive or directed to the removal of the data present on the widely leased servers. The contractual regulations will in any event, be relevant, even if from a different country than the place of establishment, in the event of a request for access by the competent authority.

With regard to this aspect, as highlighted by the analysis carried out so far, the most important factor appears to be the place of establishment of the cloud provider, the variation of which has consequences for the reachability of information by governmental and judicial authorities, law enforcement and intelligence services. Further variables may arise from the different configurations and allocations of data centers, which are often physically located in a number of locations under different jurisdictions, yet work in sync to manage the same data.[60]

A further aspect that must be taken into due consideration is the varied type of content that can be contained in the cloud: this tool, given its versatility, and the varied type of recipients (e.g. private individuals, professionals, businesses, public administrations and institutions) lends itself to storing different types of information (personal data, including special data, confidential documents, documents covered by professional secrecy, privileged documents, scientific, industrial and artistic creations, etc.) for which a high degree of security in storage and a high level of protection to prevent unauthorized access is required.

The above leads us to believe that the intervention of the judicial authorities and the forces of law and order must be surgically perimeterized, operating opportune procedural distinctions, on the basis of the type of information sought and gives rise to evaluations in law which are rather complex and which can also be very different depending on how the variables of the specific case are composed.

This complex technological and legal background undermines some of the main assumptions on which legal systems have been working for centuries and has therefore required a redefinition of the existing procedural landscape, as well as a reconsideration of the traditional methodologies and institutions for the identification, collection/acquisition, preservation and analysis of potential sources of evidence at national and international level.

We will first examine the regulatory approaches in the US and Europe. In fact, the US has recently adopted a new regulatory paradigm for access to electronic evidence, which also aims to change the relationship with third countries for the search of such evidence, and is currently home to the largest number of providers offering cloud services.

4.1. The US discipline

The US discipline is particularly relevant to the subject of this study since the largest cloud providers worldwide, and which hold important market shares in Europe and Italy, are in fact American or, in any case, use US-based infrastructures.

The US framework, normally consisting of the Stored Communications Act (SCA), was recently novated with the Clarifying Lawful Overseas Use of Data Act (so-called "CLOUD Act") which came into force on

60 As pointed out above (§ 1.3), information, already consisting of bits that can be disaggregated with the striping technique, can be distributed on various servers located in different jurisdictions, even simultaneously.

23 March 2018. This new legislation was also adopted to resolve one of the first and important litigations in the sector, the Microsoft case.

The Microsoft case

The case concerned the effectiveness of a warrant - ex §2703 of the SCA - issued before the CLOUD Act was amended - requesting Microsoft to provide access to a certain number of email accounts that Microsoft managed on its Irish servers. The question was, in essence, whether Microsoft, as a hosting provider, was obliged, once the search warrant was issued, to share communications (in this case, the email accounts and other account-related information of its customers) under its possession, custody or control, even if they were stored on foreign servers. In fact, Microsoft challenged the effectiveness of the warrant in relation to the Dublin data centers where the information was actually stored and, on that basis, sought the annulment of the measure.

A *certiorari* (review) had been sought from the US Supreme Court on the querelle, but it ultimately failed due to the introduction of §103(a)(1) of the CLOUD Act, which, by amending the SCA, made the foreign location of data irrelevant for data reachability purposes: *"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such* ***provider's possession, custody, or control****, regardless of whether such communication, record, or other information is located within or outside of the United States"*.

> *"The US discipline is particularly relevant to the subject of this study, because the world's largest cloud providers, with significant market share in Europe and Italy, are either American or have infrastructure based in the United States."*

Subsequently, under the new law, the U.S. government requested and obtained a new warrant to replace the previous one, and, therefore, the Supreme Court remanded to the Court of Appeals for the Second Circuit with instructions to overrule Microsoft's motion to dismiss, and then ordered the District Court to dismiss the case.

However, no sources have been found documenting Microsoft's actual handing over of the data, and, as will be seen, it is quite possible that enforcement and regulatory steps are still ongoing to make it possible to execute such an order - valid under US law - on servers located in the EU.

The CLOUD Act

The CLOUD Act was intended to clarify the limits and grey areas of the SCA in the face of the phenomenon of global data circulation. The SCA in fact peacefully allowed US judges to issue warrants concerning data of US subjects, held by US providers and located in US territory, but presented critical issues in the face of more complex cases which, with the evolution of technology, made it extremely easy to circumvent its application by transferring the data to other countries. In particular, the CLOUD Act sought to overcome the following problems:

1. warrants for the production of customer records held by providers subject to US jurisdiction and issued under the SCA were restricted when they concerned data of a foreign entity located outside the US;
2. the providers (and customers) subject to such orders were unclear as to the legal means to request the revocation (quash) of the warrant if they wanted to argue before the US court that it was unlawful under the law of the state where the data were physically located and the national law of the owner (either because the data were hosted by another state or because the applicable contract law was not US law);

The CLOUD Act reform thus focuses on three key points:

(i) the SCA is amended and thus introduces the principle that a company, subject to US jurisdiction, in the terms to be discussed below, may be subject to requests for production (warrants issued by an independent court) of data "**owned, managed or controlled**" by it, irrespective of where such data are stored and even if they are owned by a foreign entity;

(ii) the possibility of challenging a warrant issued on the basis of the CLOUD Act is clarified by requiring the judge who issued it to carry out a comity analysis, i.e. a particular legal analysis in which the judge must first compare the legitimacy of the warrant with any conflicting provisions of the national law applicable to the place where the data are stored and to the entity holding it[61], but then, once he has considered all the elements, he can decide for himself and carry out a sort of mediation between US law and the provisions he has analyzed or give reasons for departing from them, since he is not bound by foreign provisions; However, if the agreements described in the following point are concluded between the USA and other states, the possibility of applying for the remedy described above is removed;

(iii) the possibility for the US to automate the international procedures in question by entering into so-called "CLOUD Act Agreements", i.e. a type of agreement that introduces bilateral and automatic mechanisms of access to cloud data between the US and other states (on the basis of the grounds allowed in their respective laws), thus eliminating the possibility for the cloud provider and the customer/data owner to object to the order on the basis of the discussion of the international legitimacy of each individual warrant.

For a better understanding of the CLOUD Act, it seems useful to take into account the April 2019 white paper adopted by the US Department of Justice "*Promoting Public Safety, Privacy, and Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*". The paper clarifies which providers are included in the scope of the Act, specifying that the provisions concerning data retention and disclosure by providers are only applicable to providers of "*electronic communication services*" and "*remote computer services*". These services are defined in the Electronic Communications Privacy Act, which defines electronic communication services at 18 U.S.C. § 2510(15) as any service that provides users with the ability to send or receive electronic communications, and § 2711(2) describes remote computing services as the provision of processing and storage services to the public by means of an electronic communications system. Therefore, mailbox providers, telephone companies, social platforms, and cloud storage services fall within the potential scope of the CLOUD Act.

In conclusion, in order for the CLOUD Act to be applicable in practice to the categories of persons listed, the following conditions must be met:

- the requested data must be in the possession, management or control of the provider;
- the providers must be subject to US jurisdiction, based on an assessment that is still not free of criticism.[62]

The CLOUD Act has not modified the intrinsic characteristics of the warrant with respect to the previous discipline and, in particular, the fact that the request for access must come from the US and must concern data located in the US and under the control of a US entity remains unchanged. The reform, from this point of view,

61 By *"comity analysis"* US law means - in extreme synthesis and greatly simplifying the subject - a procedure in which the judge considers the law of a foreign state "as a courtesy". The final decision, however, remains with the US judge who is not legally bound by the foreign provisions.

62 From this point of view, there have been no changes to the provisions of the SCA, which are confirmed and, therefore, US corporations, US domiciled corporations and corporations owned by US persons can be considered as "subject to US jurisdiction" for this purpose; however, also those corporations which do not fall within the above categories, but which nevertheless have significant contacts with the US (e.g., corporations conducting a significant activity in the US) may well be considered as subject to US jurisdiction such as to make the court consider the extension of jurisdiction possible. In these terms, the criteria for defining the subjects included or that may be included are not clear-cut, but are left to a case-by-case assessment by the judge; discretionary margins are also found in the assessment of the relationships between a company and its subsidiary in terms of control of the data owned or controlled by the latter by the former. It should be noted that, in such cases, the structure and relationship between the two companies does not affect the assessment, which must in any event be carried out by the court. At the outcome of this assessment, it will be decided whether or not the warrant can be issued.

has limited itself to clarifying the content of the warrant, leaving unaltered the requisites provided by law for its release, but, as has been said, extends its territorial and subjective application.

The warrant issued under the CLOUD Act must thus, as under the previous regime, be accompanied by an affidavit - under penalty of perjury - demonstrating the "probable cause" to believe that the place subject to search will contain items that need to be seized.

The request must be enriched with additional elements, such as the alleged offense, the information subject to disclosure and the evidence for seizure. The order is subject to review by an independent judge.

Also relevant is the issue of the definition of the subject matter of the warrant, which is of particular importance for the definition of this Study. Also, from this point of view, the subject matter of warrants under the SCA has not been changed or extended in its scope, therefore:

- data collection must be circumscribed by the measure; and
- the data accessible through the provider by virtue of the warrant are those in the possession or control of the provider.

Consequently, if data are under the exclusive control of the customer and without any access by the cloud provider (e.g. encrypted with a key not available to the cloud provider), it is questionable whether they can be subject to the warrant.

The role of the cloud provider under the CLOUD Act

The cited white paper stresses the definitional consistency of the CLOUD Act with paragraph 173 of the Explanatory Report of the Budapest Convention on Cybercrime (which pursues the goal of a common policy against cybercrime) according to which *"the term "possession or control" refers to the physical possession of the data concerned in the territory of the ordering Party and to situations where the data to be produced are outside the physical possession of the person, but the person may in any event freely control the production of the data in the territory of the ordering Party (e.g., subject to applicable privileges, a person who has been served with a production order for information stored in his account via a remote online storage service must produce that information). Similarly, the mere technical ability to access the data remotely (e.g., the ability of a user to access via a link data that is not within his or her legitimate control), does not constitute "control" within the meaning of this provision..."*.

The issue of data control and possession is of primary importance[63], considering the possible implications due to factors such as the purposes for which the data is held by the provider. There are obvious differences depending on the different reasons for which the data are at the provider's disposal. As already highlighted in §3.2., it is in fact necessary to make a distinction on the basis of the service provided by the provider: if the data is processed for the purposes of modification, processing or implementation, it is possible to assume control and possession of the data by the operator; if, instead, the information collected on the cloud is stored for storage purposes only, it is assumed that it is outside the possession and control of the provider. In the latter case, the cloud provider could not have access to the content, which is only available for access by the user.

Moreover, the conviction that these data are not available to the provider is reinforced by the fact that encryption techniques are often - or rather, almost always - used in these cases, aimed at ensuring unambiguous access to the client, which, in some cases, in addition to ensuring access to the information, allow the prodromal recomposition of the fragments of the same, which are distributed on different data centers. On this point, it is worth clarifying that not even the post-CLOUD Act SCA warrant can go so far as to require the provider to carry out the laborious and improbable decryption of the files; indeed, the white paper expressly excludes this possibility.

In conclusion, the encrypted data can neither be accessed nor reached by the provider and is therefore outside the provider's possession or control, rendering the provision of the CLOUD Act inapplicable.

63 See above, § 2.1.

As to the type of data that can be extracted, these, if reachable, may potentially include the content of communications, associated metadata, subscriber information and data stored on behalf of the user.

Access to data belonging to non-US citizens and CLOUD Agreements

A final issue, which then opens up to the second topic addressed by the CLOUD Act, concerns access to data belonging to non-US citizens/residents (including, precisely, Italian and European citizens/residents). It should be recalled that the measures based on the CLOUD Act consider the citizenship or residence of the client as a determining element, whereas the location of the data is of less relevance.

As we have just demonstrated, companies subject to US jurisdiction would have to peacefully comply with a warrant involving data of non-US citizens/residents if there is a CLOUD Agreement with the country where the data are located. Conversely, in the absence of such an agreement and if the warrant is in conflict with the law of the country of destination, the effectiveness of the measure could be questioned to the extent of restricting its claims to comply with the law of destination (by way of quash request through comity analysis).

Moreover, if data were to be stored in multiple states and in the absence of relevant CLOUD Agreements, the enforcement of a warrant could be opposed by the cloud provider and the owner with multiple comity analyses, making it quite difficult, also by virtue of the fact that the multiple parts of data subject to the jurisdiction of different states could be subject to different decisions.

Alternatively, if the instruments provided by the CLOUD Act were not to be used, the prosecuting authorities would have to resort to more traditional procedures such as negotiating in good faith or re-submitting the request on the basis of a Mutual Legal Assistance Treaty (MLAT); however, these are complex instruments and therefore tend to be seen as absolutely secondary.

CLOUD Agreements and MLATs

It is therefore understandable that the possibility of concluding agreements on the basis of the CLOUD Act is the second key element of the reform.

The conclusion of such agreements is conditional on the US[64], recognizing that the legal system of the contracting state offers a standard of protection for privacy and civil liberties at least equivalent to that of the United States.

At the time of writing, there are no EU Member States that have concluded CLOUD Act Agreements with the US.

The only such agreement to date was signed by the UK in October 2019[65] and immediately raised questions in the Euro Parliament about its legitimacy[66]. Following Brexit, there is also likely to be a need for its revision as it refers to mechanisms under the EU-US Conventions on the transfer of crime prevention data[67]. Overall, the Agreement outlines a mechanism of reciprocal safeguards in the event that the requested transfers (in any case, only of data related to criminal investigations) are contrary to what are defined as "essential interests" of the contracting States.

> *"Under the CLOUD Act, any company subject to US jurisdiction may be subject to requests to produce data owned, managed, or controlled by it, regardless of where that data is stored and even if that data is owned by a foreign entity."*

However, there is no doubt that a State could not ratify such an Agreement in violation of its own provisions (in the case of EU Member States, for instance, the GDPR).

The CLOUD Act also envisages MLATs as a further mechanism to cover areas not covered by the Agree-

64 This is a certification, to be carried out in advance, by the US Attorney General of Congress.
65 See Agreement of 3 October 2019 between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, available online at https://cli.re/jJ7Z3D.
66 See https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html
67See Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses done at Amsterdam; 2 June 2016, available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.

ments. The peculiarity of these agreements, stipulated through ordinary diplomatic channels in the form of international treaties, lies in the fact that they do not allow, in principle, to recognize - as instead happens in the CLOUD Agreements - the automatic effectiveness of orders of the other contracting State but only the possibility of forwarding to the competent Authorities of the State a request to be validated but which could also be refused.

Despite the fact that the laws of the countries with which the Agreements are signed must be at a level with the standards of the United States, an assessment that, as mentioned, will be carried out ex ante, the procedure for the issuance of the measure, corresponding to the US warrant, must therefore, in the case of the MLAT, follow the procedure provided for by the national law of the other country in order to arrive at the final measure and request, and obtain, the information directly from the provider.

MLATs may therefore occur in the area of measures to combat serious crimes, in the case of criminal proceedings, for the prevention, detection, investigation or prosecution thereof.

Criticism of the CLOUD Act

The passing of the CLOUD Act has been met with severe criticism in Europe and worldwide.

These criticisms concern, for the most part, the excessive simplification of the procedures and the reduction of the guarantees for the protection of fundamental rights that is brought about when the CLOUD Agreement is concluded, which are considered to be worse than the regime previously ensured by the MLAT provision alone, which was in any case valid even before the CLOUD Act.

The effect of this is to reduce the effectiveness of provisions of third States designed to protect personal data and to abolish, in practice, the possibility of objecting by requesting a comity analysis and, with it, consideration of the reasons under the law of the third State potentially impeding the transfer[68].

The analysis of the legislation also shows that the lack of a procedure providing for any official communication or notification to the State where the data are stored or to the State of the data subject's nationality of the initiation of data request procedures, even when access is concluded or when, in any case, investigations would not be compromised, has led, for instance, some large cloud providers to introduce a policy[69] of notifying the customer of requests received under the CLOUD Act.

Concern was also expressed by the European Parliament[70] about the scope of the processing of personal data, with particular reference to Article 48 of the GDPR, which makes the recognition of decisions or judgments of foreign authorities ordering the transfer or communication of personal data subject to their being based on an MLAT Agreement in force between the requesting country and the European Union (or one of its Member States) and not on a CLOUD Act Agreement. In this light, the CLOUD Act does not seem to offer the necessary comfort for the court order to be considered in line with the GDPR. Indeed, in the absence of an MLAT agreement or other legal basis under the GDPR, the provider could not lawfully disclose and transfer the personal data requested by the US. Moreover, the Privacy Shield - recently invalidated by the CGUE's Schrems II judgment - would not even have seemed applicable to that transfer, as it applied to the transatlantic transfer of personal data for commercial purposes.

The EDPB and the European Data Protection Supervisor (EDPS), who intervened on this issue, agreed on the need to at least recognize and enforce the US CLOUD Act on the basis of an international agreement containing procedural and substantive safeguards to align data transfer protection levels with European standards[71]. In this way, the legal basis for the processing would be the legal obligation recognized by Article 6(1)(c) of the GDPR.

68 See Schwarz-Peifer, Data Localization, Under the CLOUD Act and the GDPR, Computer Law Review International, 2019/1.
69 See White Paper Google on Data residency, operational transparency,and privacy for European customers on Google Cloud, available online at: https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf?hl=cs.
70 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, nn. 27 e 28 available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN.
71 See the joint EDPB/EDPS response of 12 July 2019, accessible at the following link: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_de in which the EPDB concluded that: "*service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the US on such requests*".

The above mentioned discrepancies appear to be the symptomatology of a serious tension between the CLOUD Act and some fundamental rights recognized at European level, among which in particular the right to privacy, which is identified by the primary law of the Union and, in particular, by the European Charter of Fundamental Rights of the European Union (Articles 7 and 8), of which the GDPR represents the normative precipitate, as well as by the European Convention on Human Rights (Article 8) as declined by the case law of the CGUE and the European Court of Human Rights.

The Council of Bars and Law Societies of Europe (CCBE) has also expressed[72] concern about information that can be extracted from communications between lawyers and clients. Confidentiality is an essential element of professional ethics and is generally recognized as a corollary of the right to defense. The indiscriminate and unprocedural seizure of privileged or privileged material is a serious violation of the rights of persons subject to disclosure, especially if the lawyer is not informed of the seizure.

Therefore, also in this respect, the CLOUD Act is potentially detrimental to the rights of individuals to a fair trial. Indeed, the very failure to provide for the inadmissibility of evidence gathered in this way suggests that the provision is incompatible with the principles referred to above.

The transnational relevance of the provision leads to a reflection on the possible implications in terms of international comity, which the CLOUD Act seems to solve in an authoritative way and according to logics aimed at expanding jurisdiction, not always properly compatible with the legal systems with which it relates.

Developments in judicial cooperation

The concerns that have been expressed in the European context, from many sides, are partly reflected in the recommendation for a Council[73] decision authorizing the opening of negotiations for an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters.

> *"The compatibility of orders issued under the CLOUD Act with the requirements of the GDPR must be verified."*

An earlier agreement on transatlantic cooperation in criminal justice and the fight against organized crime and terrorism was signed in June 2003 and entered into force in February 2010. That agreement was then reviewed in April 2016.

For its part, the EU would like to address the issue of cross-border access to data and metadata from the perspective of protecting European rights and values by incorporating both the EU-US Data Protection and Privacy Agreement of February 2017 and the US Judicial Redress Act into the new Agreement, extending the guarantees of the US Privacy Act of 2016 to European citizens.

In particular, according to the Council, "*The agreement will have to respect fundamental rights, freedoms and general principles of EU law as enshrined in the EU Treaties and the Charter of Fundamental Rights, procedural rights including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defense, the principles of legality and proportionality of criminal offenses and penalties, and any obligations incumbent on judicial or law enforcement authorities to that effect. As regards the necessary data protection safeguards for personal data transferred from the EU to the US, the applicable provisions of the EU-US Privacy and Data Protection Agreement will be complemented by additional safeguards to take into account the level of sensitivity of the categories of data concerned and the specific requirements of the transfer of electronic evidence directly from service providers.*"

Formal negotiations between the EU and the US began in September 2019 and, however, have not yet been concluded.

72 See the position paper of 28 February 2019 accessible at the following link: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf.
73 Act of 5 February 2019, accessible at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0070.

4.2. The European discipline

The European scene appears to be in flux. Over time, periodic reforms of new cooperation mechanisms have been put in place with the aim of adapting investigations to the digitalization of society and the economy, speeding up cross-border electronic evidence collection procedures and bringing fragmented national procedures back into line.

First and foremost, Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in criminal matters (EIO), which is a European version of the international letter rogatory. An international letter rogatory consists of an order from one judicial authority to another, located in a different jurisdiction, to execute a procedural act related to the needs of criminal proceedings or a criminal trial in progress before the person making the order. The content of the letter rogatory can obviously be the activity of obtaining evidence, which includes requests for access to data contained in a server.

For the sake of completeness, it should be remembered that the subject of mutual assistance is governed first and foremost by the European Convention on Mutual Assistance in Criminal Matters, signed in Strasbourg on 20 April 1959 and, in the European context, by the New Convention on Mutual Assistance in Criminal Matters between the fifteen Member States of the European Union signed on 29 May 2000.

With strict reference to cooperation against cybercrime, mention should also be made of the Council of Europe Convention on Cybercrime of 2001 (the so-called Budapest Convention), concerning, *inter alia*, coordinated procedures for obtaining electronic evidence. The Budapest Convention, which has been ratified by a large number of Member States, provides for faster investigations, given the nature of the evidence and its rapid circulation.

However, the current legal instruments still seem to be blunt weapons to counter the widespread parcellation of information that characterizes the structural model of the technology used by clouds. Indeed, if on the one hand there is a problem of timeliness and duration of requests made to foreign authorities, on the other hand, these may not be conclusive, if one considers that the data, or rather the related bits, may be distributed in different locations and subject to different jurisdictions. Moreover, here again, the dilemma arises as to whether the data sought can be considered as being in the possession and control of the provider, if the latter does not have the possibility to overcome the encryption system in order to reassemble the data and be able to view it.

Recently, the introduction of new measures in Europe that do not take into account the place where the data are stored and address the request directly to the cloud provider is being considered. The need arises from the increasing number of investigations that require the provision of evidence held on foreign servers, even if it relates to crimes committed entirely within the territory of the prosecution.

In this respect, it should be noted that a proposal for a Regulation for European orders for the production and preservation of electronic evidence[74] has been in the pipeline since April 2018, which will operate in the criminal field. The instrument should complement the aforementioned EIO to simplify the collection of evidence held in another jurisdiction. In particular, according to the proposal, the order to obtain electronic evidence (so-called “e-evidence”) would be mutually recognized - through validation - between Member States, involving the foreign authority only in case of necessary enforcement.

However, it should be noted that despite the procedural simplification, which seems to be based on the US model, the Regulation is still a source of secondary law and, therefore, must comply with the primary legal substratum, which outlines the fundamental rights of the EU.

The proposal for a regulation also addresses the issue of reciprocity obligations with third countries, but it will necessarily have to deal with the evolution of the negotiations between the EU and the US on the drafting of the Agreement, which have taken place since the Commission presented its proposal.

74 Proposal of 17 April 2018 accessible at the following link: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

Also to be carefully considered is the aforementioned Regulation (EU) 2018/1807 for the free flow of non-personal data, which aims to remove the barriers that currently prevent the free cross-border movement within the EU of non-personal data, i.e. data that do not relate to identified or identifiable natural persons but, at the same time, seems to foreshadow an EU regulation of the legal reachability of this type of data.

The new provisions contained in Regulation 2018/1807 complement those providing for the free movement and portability of personal data within the EU contained in the GDPR, and together with the latter, in the intention of the European legislator, they would like to contribute to the creation of that "common European data space" desired several times by the European Commission itself[75], as one of the prerequisites for the development of the single digital market and the data economy within the Union. The Regulation 2018/1807 in question mainly identifies two categories of obstacles to the free movement of non-personal data: these are vendor lock-in practices in the private sector and data "localization" obligations[76] put in place by the authorities of individual Member States. The latter are the ones relevant to the issue of reachability. They can be identified in Member States' laws that impose (a) obligations to localize data for processing purposes in a given territory, or (b) specific requirements that make it more difficult to process data outside a given territory.

The Commission has therefore identified a number of restrictions on where data are stored or processed, affecting data mobility, in different areas, for example:

- supervisory authorities recommending that financial services providers store data locally;
- rules on professional secrecy (e.g. in the case of the health sector) that require data to be stored or processed locally;
- general rules requiring local storage of information generated by the public sector, regardless of its sensitivity;
- rules requiring the use of technological devices that are approved or certified in a particular member state (see recital (4) of the Regulation).

In the face of data localization obligations, such as those just described, Regulation 2018/1807 provides that national rules imposing localization obligations are unlawful, except for reasons of public security and within the limits of the principle of proportionality and, above all, provides that "competent authorities"[77] must be guaranteed access to data stored or processed in another Member State (see Article 5).

It applies to processing activities of electronic data other than personal data in the Union, which are provided as a service to users (natural or legal persons, including public authorities and bodies governed by public law) residing or established in the Union, whether or not the service provider is established in the Union; or carried out by a natural or legal person residing or established in the Union.

In the case of a dataset composed of both personal data and non-personal data, Regulation 2018/1807 applies only to the part of the dataset containing the non-personal data, whereas in the event that the personal and non-personal data in a given dataset are inextricably linked, Regulation 2018/1807 is without prejudice to the application of the GDPR.

Recital (9) of Regulation 2018/1807 specifies that the expansion of the Internet of Things, artificial intelligence and machine learning are important sources of non-personal data, as in the case of their use in automated industrial production processes.

75 See European Commission Communication of 2 July 2014 "Towards a thriving data-driven economy", as well as Communications of 25 April 2018 and 15 May 2018.
76 Article 3, nr. 5, defines an obligation to locate data as "*any obligation, prohibition, condition, limitation or other requirement, provided for by the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practice in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which requires the processing of data to be carried out on the territory of a particular Member State or which impedes the processing of data in another Member State*".
77 Defined by the Regulation as "an authority of a Member State or any other body authorized under national law to exercise a public function or to exercise public authority, which is entitled to obtain access to data processed by a natural or legal person for the purpose of carrying out its official functions, as provided for by Union or national law". As we can see, the definition leaves the door open to the fact that the Authority can also be a foreign body, provided it is "authorized".

The same recital (9) gives some specific examples of non-personal data: aggregated and anonymized datasets used for metadata analysis, data on precision agriculture that can monitor and optimize water and pesticide use, and data on maintenance needs of industrial plants.

Recital (9) further specifies that, should technological progress allow anonymized data to be transformed into personal data, they would be considered as personal data, with the consequent application of the GDPR.

Finally, art. 2, paragraph 3, of Regulation 2018/1807 specifies that the same does not apply to activities outside the scope of Union law. On this point, recital (12) reminds us that, under Article 4 of the Treaty on European Union, national security is the exclusive responsibility of each Member State.

4.3. The national discipline

Turning to the domestic context, it is well to recall Article 234-bis of the Code of Criminal Procedure, according to which: "*The acquisition of documents and computer data stored abroad is always allowed, also different from those available to the public, subject to the consent, in this last case, of the legitimate owner*". The provision reinterprets Article 32 of the Budapest Convention and operates without the necessary rogatory or EIO. There appear to be no limitations as to the offenses for which the Article is applicable.

The field of application intersects the subject matter of this Study with reference to computer data stored abroad and not accessible to the public, precisely because they are organized according to the cloud model. With reference to this last observation, it must, however, be specified that if the contents relate to archived private communications (for the flow of information, the interception *ex art. 266-bis* c.p.p. should apply) or, however, that concern metadata, it would be necessary, for the acquisition, once again, an order of the judicial authority and the request by means of international rogatory, or EIO, making the provision less incisive than it appears to be.

The ambiguous reference to the "consent of the legitimate owner" reinforces the perplexity about the simplifying functionality of the provision in question, an evanescent concept that certainly cannot be attributed unreservedly to the cloud provider, unless it is defined as such in the contract with the user. On the other hand, the parallelism with the concept of owner as identified in the GDPR would be irrelevant and limited to personal data only. Equally problematic would be to consider the subject under investigation (or defendant) as such, since a paradoxical consent would have to be given by the latter.

In any event, the provision in question has a little impact with respect to modern storage technologies which, as has been said several times, tend to provide for a fragmented and widespread location of data, making it difficult to identify the foreign country to which the request should be addressed, since the request should be addressed to a plurality of recipients - which are also difficult to identify - who in most cases are not located in the same country as the provider's headquarters.

CHAPTER 5
CONCLUSIONS

5.1 The overall picture

The Study pointed out that the choice of cloud provider must be subject to a specific assessment if the data entrusted to the cloud are strategic, or in any case relevant, for the company or organization in question.

The criticality of data does not only relate to the personal nature of the data, but any industrial value or public value that the data may have. From a business perspective, non-personal data, particularly corporate data, may be more sensitive to be entrusted to the cloud than personal data because of their economic value and the recent EU rules that seem to open up new mechanisms for cross-border accessibility of such data, which are not possible for personal data. This concerns above all the B2B and corporate market, but could also be extended to the consumer and SoHo markets. Indeed, any private user should be well aware of the fate and status of his or her own data once they are placed in a cloud system, especially since the cloud provider holds contractual power in this relationship.

Cloud outsourcing brings with it undeniable and far-reaching advantages in data management that a local infrastructure could hardly provide as an alternative. These advantages are not only economic, but also and above all in terms of security, infrastructure scalability and the possibility of sharing and processing data. But the paradigm shift from on-premises to the cloud brings with it additional issues and, in particular, the potential risk of losing control over one's own data, not only in technological but also in legal terms.

In the current context, precisely because of the prospect of such enormous advantages, but in the absence of a well-considered assessment of collateral risks and in the face of legal instruments of contrast that are still immature, there is a risk that the decision to outsource data to the cloud may be taken without due assessment and attention from a contractual and regulatory point of view, and this, in particular, with regard to the issue of "reachability", which was the subject of analysis in this Study.

The normative framework that is being outlined at an international level - and of which the American CLOUD Act constitutes one of the most advanced offshoots - provides for a regime whereby the public authorities that have jurisdiction over the cloud provider to which the data is entrusted have, under certain conditions, the possibility of "reaching" such data even if it falls under the ownership of a subject that does not fall under their jurisdiction and even (and here falls the main novelty of the CLOUD Act) when it is not physically hosted in servers subject to the jurisdiction of the State that issued the order. This possibility, which is not limited to the US system but is progressively spreading in the various world systems, including the European Union, must however be put in the right perspective.

In fact, it must be considered that there is no possibility of indiscriminate access by public and governmental authorities to data outsourced in the cloud, except in systems that do not respect human rights. The access of the public authorities to the data held by the cloud providers remains regulated by the ordinary national or international legal procedures, in the latter case where such data concern subjects - private or corporate - who are citizens of other legal systems: for example, EU citizens are protected by the GDPR with regard to personal data, while the use of data in criminal proceedings, as mentioned above, is regulated by the Budapest Convention. States have long since equipped themselves with tools to access their citizens' and companies' data managed in the cloud by their national providers in circumstances that the law considers lawful (national security, crime prevention, crime investigation, counter-terrorism, etc.).

Therefore, entrusting data to the cloud at national level does not per se entail excluding them from the "reachability" of one's own public authorities in circumstances where such data would have been "reachable" anyway had they remained with the data controller or, even, of foreign authorities authorized by the State of residence, in circumstances where national law does not offer specific grounds for protection (e.g. non-personal data and not protected as intellectual property or otherwise and specifically contracted as being unavailable to the cloud provider).

5.2 Hypotheses of criticality regarding the data reachability, and related recommendations

There are, however, critical aspects of "reachability" that concern those circumstances in which a foreign State, which would not have been able to "reach" the data if it had remained in the local management of the owner or in a national cloud, in certain circumstances such as those described in Chapter 4, could, for the sole reason of entrusting the cloud to a provider subject to its own jurisdiction or to the jurisdiction of a State with which the State has stipulated international agreements, be able to "reach" the data of a subject even if located outside of its own territory. This is a scenario that can significantly affect the commercial choices of companies and public procurers, creating serious barriers to the deployment of cloud services globally.

In such cases, the solution identified in this Study consists in negotiating, through a careful analysis and negotiation (where possible) of the contract and, in particular, of the technical annexes such as the DPA, the SLA and the security annexes, a series of precautions and, in particular:

> *"With the US CLOUD Act, public authorities with jurisdiction over the cloud provider to whom the data is entrusted can, under certain conditions, "reach" that data even if the owner does not fall within its jurisdiction and even - this is the main innovation of the CLOUD Act - if the data is not physically hosted in servers subject to the jurisdiction of the State that issued the order."*

- data storage that is distributed, either fixed or variable, across multiple jurisdictions, preferably in EU Member States to ensure that data is managed with the protections provided by the GDPR and that these protections are enforced by state law, and not by conventional provider obligation;
- the encryption of the data at the cloud provider, with the customer's key and not available to the cloud provider (except where it is essential that the cloud provider has access to the data), so as to ensure that, even where there is an order to show the data, that order can only relate to encrypted data;
- the application to cloud contracts, where there are no specific requirements, of the contract law and dispute jurisdiction of EU states, so as to ensure that any disputes on discovery orders take place on the basis of EU law and before EU courts;
- adequate pre-contractual information, also through the AUP, about situations, services and types of data that the cloud provider considers accessible to its public authorities and on the basis of which types of orders (on which also *infra*);
- obtaining specific guarantees from cloud providers regarding information and the possibility to intervene in case of requests for access to cloud data by public authorities;
- obtaining information from the cloud provider prior to the conclusion of the contract on how it has behaved in the face of requests from public authorities for access to cloud data in services similar to those proposed, and periodic reports on the matter;
- obtaining guarantees about any subcontractors, who must use the same territories, be of the same nationality (or, in any event, of nationalities authorized by the Client) and offer the same contractual guarantees;
- the contractual provision on how to handle the return of the data if, as a result of legislative changes, the contractual guarantees referred to above can no longer be met by the cloud provider, or if the latter can no longer keep the data by order of the foreign authority or by decision of the provider himself.[78]

Only in the next few years will we know whether the international framework is capable of creating a network of agreements between States, and in particular between large economic macro-areas, which will make automatic the operation of data apprehension at international level on the basis of common and harmonized principles. The recent events on the subject of data flow, and in particular the cancellation of the Privacy

78 See for example the Parler / AWS Amazon case, already cited.

Shields, have on the one hand created great uncertainty in the sector, and on the other made companies and governments more responsible, as they have understood the need to create global data governance.

At present, even provisions such as the US CLOUD Act, although “theoretically” efficient, suffer from considerable application complexities due to the need to arrive at the execution of the data exposure warrants, verifying their legitimacy on a case-by-case basis.

It is possible to counter the conclusion of such automatic agreements with work aimed at clarifying in detail, for the benefit of the judges called upon to interpret the situations and of the cloud providers/entities called upon to assess any opposition, what the situations are of the illegitimacy of the requests, so as to form a base of cases which, to date, is lacking and which, in turn, will certainly provide ideas for improving what is provided for in the contractual agreements.

In this respect, the cloud providers themselves can work concretely in terms of pre-contractual information, specifying not only what the AUPs are, but also the situations, services and types of data that they consider accessible to their public authorities and on the basis of what types of orders, while avoiding general clauses providing for obedience to “any order” issued “under the applicable law”, since the issue of whether or not data can be accessed by external entities, in a society increasingly based on data, cannot but be an issue to be clarified with extreme precision and transparency.

A remedy could be found in the study of a cloud “standard contract” and a code of conduct - also international - that could be adopted as best practice by any cloud provider wishing to present itself to the customer by offering the broadest guarantees of cross-border data protection and containing commitments verified by third parties in this sense. Even in the face of such a mechanism, however, it has been seen that some imperial “reachability” may be unavoidable if the data are processed in territories subject to regulations providing for the subjection of the cloud providers operating there and in possession of the data to imperial procedures of making the data available to requesting authorities - judicial or governmental - without adequate possibilities for the data owner to object.

Moreover, as highlighted in the document, the contractual detail - which could become a “code of conduct” - becomes more essential than ever and an instrument of guarantee for both the user and the provider in certain cases - now more topical than ever - to regulate procedures of inhibition, restitution and deletion of the data that the user entrusts to the cloud provider, and this both in the face of orders from the competent Authority, and in the face of self-defense initiatives by the cloud provider.

AUTHOR PROFILES

EUGENIO PROSPERETTI

Eugenio Prosperetti is a lawyer and university lecturer at the LUISS "Guido Carli" University in Rome. He has been dealing with the legal issues of new technologies for over 20 years, assisting national and multinational companies on regulatory, contractual and judicial issues concerning services, contracts and compliance in information technology markets.

Studies

- 2005: PhD in commercial law with a thesis on "La regola del rapporto tra creatore e utilizzatore di software" (Faculty of Economics, University of Rome "Tor Vergata").
- 1998: Law degree with 110/110 at the University of Rome "Tor Vergata".

Professional activity

- Member of the Rome Bar Association, qualified as a lawyer, higher jurisdictions.
- After several years of experience in international firms since 1998 (Baker & McKenzie - associate and Portolano Colella Cavallo Prosperetti - partner), in 2005 he took over the management of his own law firm in Rome where he assists Italian and foreign clients, including public administrations, in matters including information technology regulation, complex cloud platforms, privacy and data management, electronic communications, digital payment systems, data management and services in artificial intelligence systems, blockchain systems, antitrust in digital platforms, antitrust compliance, e-government platforms, e-commerce, unfair commercial practices proceedings, public procurement. It also assists clients in related administrative and civil litigation and with independent authorities.

Institutional activities

From May 2017 to June 2019: 25-month assignment as legal advisor Agid - FICEP project (First Italian Crossborder Eidas Proxy) for cross-border interoperability of electronic identities.

- 2017: member of the Agid Task Force on Artificial Intelligence.
- 2016: member of the working groups that studied and drafted the reform of the Digital Administration Code (implementing art. 1 L. 124/2015 - P.A. reform) at the Ministry of Public Administration and called upon to participate as a support technician in the meetings of the Agid Steering Committee on the same issues, received thanks from Minister Madia for his work.
- 2014-2015: member of the Permanent Table for Innovation and the Italian Digital Agenda at the Presidency of the Council of Ministers established under Article 47, Law 5/2012, appointed by Prime Minister's Decree.
- 2013-2014: participated as a guest in the working groups at the Presidency of the Council of Ministers that studied and then drafted the legislation on SPID - Sistema Pubblico dell'Identità Digitale (convened as a technician at all meetings, and was thanked by the then commissioner Francesco Caio for his participation and contribution).
- 2010: Member of the working group in charge of one of the Work Packages of the study ISBUL - Infrastrutture a Banda Larga e Ultra Larga promoted by AGCOM (formally reported among the Authors of the Study).
- 2007: Appointed by a special Ministerial Decree, he was a member of the Technical Secretariat of the

Minister of Communications, Hon. Paolo Gentiloni, where he dealt with the implementation in Italy of electronic communications regulations and regulations implementing international treaties on computer security and digital copyright, and was a member of the commission that drew up the Italian wi-max/BWA call for tenders and specifications; he received praise from the Minister Paolo Gentiloni for his work.

- 2007: Member of the Committee for the Protection of Intellectual Property at the Presidency of the Council of Ministers.

Main academic activity

- since 2021, contract professor of "Algorithm and Data Management Law" at the Faculty of Law of the University LUISS "Guido Carli" of Rome;
- from 2015 to 2020 Adjunct Professor of Legal Aspects of Information Technology at the Faculty of Law of the University "LUISS Guido Carli" of Rome;
- since 2017: eligible for appointment as professor of commercial law (IUS/04 - SSD 12/B1);
- He is the author of numerous publications in scientific journals and collective volumes; among the topics covered: software contracts, cloud contracts, legal regime of big data, on digital works, digital rights management and the monographic essay "La circolazione dell'opera digitale tra regole e mercato" (Giappichelli, 2012).

INNOCENZO MARIA GENNA

Innocenzo Genna is a lawyer specializing in European policies and regulations for digital, competition and liberalization. With over 25 years of experience in the field, he currently works in Brussels, where he holds association positions and assists Italian and foreign operators.

Studies

Innocenzo Genna has a degree in law, two master's degrees in European law and a French diploma in comparative law:

- he was an Erasmus student from 1989 to 1990 in Bremen (Germany), and in the same period, he privately attended courses in West Berlin at the Freie Universität;
- graduated in law in 1991 in Macerata with honors (110% cum laude), with a thesis in international law on the legal status of Berlin until German reunification;
- in 1992 he obtained a Master's degree in European Law (LLM) at the College of Europe in Bruges, with a thesis on "Droit communautaire et privatisations";
- in August 1993 he obtained the Diplôme supérieur en droit comparé issued by the International Faculty of Comparative Law, University of Strasbourg, completing a series of courses that began in 1991 at various academic venues, i.e. Trier, Strasbourg, Trapani and Florence;
- in September 1993, he obtained his Magister Iuris (LLM) from the Faculty of law at the University of Trier (Germany).

Professional experience as a lawyer

He qualified as a lawyer in 1995, but his professional experience in the legal field started already in 1992. He has worked on both European law and national and comparative law, with a particular focus on digital, privacy, antitrust, commercial and corporate law:

- in 1992, he was a trainee at the Tizzano & Pappalardo law firm in Brussels;
- from March to September 1993, he was a trainee at the Court of Justice of the European Communities in Luxembourg;
- from October 1993 until May 1997 he practiced law at the Bernini Law Firm in Bologna;
- from June 1997 until March 2002 he practiced law at the Ughi e Nunziante law firm in Rome, where he became a partner in 2000;
- in April 2002, he became manager and head of the legal department at the Tiscali Group in Cagliari and Milan, where he also started to deal with European institutional relations, until 2006;
- from 2004 to 2006, he was a member of the Ministerial Committee on Internet and Minors.

Professional experience as a lawyer and in European public affairs

- Since mid-2006, Innocenzo Genna has moved to Brussels where he has been working in a specialized way on European digital law, assisting Italian and European companies and holding various association roles):
  - in 2007 he was appointed president of ECTA (the European association of telecom new entrants), a position he held until 2009;
  - since 2010, he has founded and led Genna Cabinet Sprl, a European strategy and public affairs consultancy in the field of digital and liberalization;
  - is Vice-President of Euroispa, the European association of Internet Service Providers, on whose board he has sat since 2007;
  - since 2016 he has been Vice-President of MVNOEurope, the European association of MVNOs;
  - served as a Board member of the EIF (European Internet Forum) at various stages, from 2004 to 2006, and then from 2014 until 2021;
  - since 2018 he has been a member of the Communications Committee of IBA (International Bar Association) where he serves as EU Liaison Officer.

Publications and miscellaneous

- Innocenzo Genna edits the professional blog dedicated to the European digital world Radio Brussels Free (https://radiobruxelleslibera.com).
- He is the author of several publications on numerous digital-related topics. He also writes about innovation and digital media for La Stampa, Il Foglio, Il Post, Wired, Huffington Post and Agenda Digitale.
- He is co-founder of Digit@talians, the network of Italian digital professionals. In this capacity he has organized and managed, from 2014 to date, numerous events dedicated to Italy and digital.
- He is co-founder and president of the association Allez les Marche! - Marchigiani in Brussels.

with the collaboration of

GIULIO PASCALI

Graduated in Law at the University "LUISS Guido Carli" in Rome, he obtained at the same University a Postgraduate Diploma in Law and Management of Intellectual Property, Competition and Communications. A lawyer since 2012, she works with Studio Prosperetti in Rome, dealing with Privacy, Cloud Contracts and Procurement of Cloud Services, Advanced Electronic Communication Services and Telemarketing, Copyright, Fintech and Innovative Start-Ups.

He collaborates with the chairs of "Informatica Giuridica", "Legal Aspects of Information Technology" and "Algorithm and Data Management Law" at the Department of Law of LUISS Guido Carli and the chairs of "Informatica Giuridica" and "Diritto dell'Amministrazione Digitale" at UniTelma Sapienza.

DAVIDE TUZZOLINO

Lawyer, he has been working with Studio Prosperetti since 2020 where he focuses on data privacy, cloud contracts and information technology litigation. He has gained particular experience in the field of personal data processing, cloud and digital intellectual property also in the context of academic research and is actively working on some forthcoming publications in these fields.

Davide is in the second year of his PhD at the European University of Rome and is an assistant professor of Private Law at the same University.

He is also an assistant professor of Legal Informatics at the LUISS Guido Carli University in Rome.

He is a fellow of the Italian Academy of the Internet Code (IAIC).

He graduated from the University of Rome "La Sapienza", obtained a diploma of specialization for the legal profession from the European University of Rome and a second master's degree in European Private Law at the University of Rome "La Sapienza".

NOTES

1 Among the most recent data, see Synergy Research Group, First quarter 2020, http://www.globenewswire.com/NewsRoom/AttachmentNg/5d1edd1e-dc3c-4847-9fc0-23-a5e0eb20d5/en.

2 Definition set out at https://cloud.italia.it.

3 Cloud-based data management can offer the possibility to host data in infrastructures with levels of security otherwise inaccessible to small and medium-sized businesses/professional offices, and managed by specialized personnel.

4 National Institute of Standards and Technology, US Department of Commerce; The Nist Definition of Cloud computing, Special Publication 800-145, September 2011. Available at the following link https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial-publication800-145.pdf.

5 The "leap forward" that occurred in Italy due to Covid is well represented by Eurostat statistics, Cloud computing - statistics on the use by enterprises, 19 January 2021.

6 Eurostat data: Use of cloud computing services in enterprises, 2020.

7 2019-2020 edition of the Cloud Transformation Observatory of October 2020; see the press release accessible at the following link: https://www.osservatori.net/it/ricerche/comunicati-stampa/cloud-italia-mercato-2020.

8 Speech by Minister Paola Pisano, at the Gaia-X Summit online, 19 October 2020, available at the following link here: https://innovazione.gov.it/assets/docs/2020-11-19-intervento-ministra-pisano-a-gaia-x-summit.pdf.

9 Adopted by DPCM of 17 July 2020 and available at the following link: https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_l_informatica_nella_pa_2020_2022.pdf.

10 Version adopted in 2016, and following comments from the European Commission, and available at the following link: https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf.

11 The 3 elements of the strategy are available at the following link: https://cloud.italia.it.

12 See AgID Circulars No. 2 and No. 3 of 9 April 2018. See also: https://cloud.italia.it/marketplace/ .

13 The Marketplace also indicates how a specific service can be acquired by an administration by referring to the available procurement tool (the www.acquistinretepa.it portal) to proceed with the acquisition.

14 See https://www.consip.it/attivita/gara-spc-cloud-disponibile-la-documentazione and thematic websites of awarded framework contracts: lot 1: https://www.cloudspc.it/ lot 2: https://www.spc-lotto2-sicurezza.it/ lot 3: www.spclotto3.it lot 4: www.spclotto4.it.

15 Beyond the mentioned contractual tasks towards the PA, the main purpose of these local resellers is to provide sales force on the territory and ensure the integration of services (both cloud and others). However, there may be little possibility for these small resellers to influence the policy, technology and governance of cloud services (e.g. security policies, territorial distribution of data, configuration of services), which remain mainly in the hands of the global operator. This should be assessed on a case-by-case basis. It is also worth noting, in the national context, indicating the growing importan-

ce of national realities capable of interacting with large cloud operators (in this case Google), the very recent establishment of the new company Noovle Spa dedicated to cloud enabling activities into which the Telecom Italia group's data center network has converged.

16 See http://www.politicheeuropee.gov.it/it/comunicazione/approfondimenti/pnrr-approfondimento/.

17 Definition taken from http://www.dei.unipd.it/~dinunzio/fdi-2014-2015/04_dati_informazioni.pdf.

18 Regulation (EU) 2014/910 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Art. 3 para. 35.

19 See chapter 2 of the Study.

20 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019, Articles 1 and 2.

21 Article 2 (1) of the "Proposal for a Regulation of the European Parliament and of the Council on European data (Data Governance Act) {SEC(2020) 405 final}: "data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording;".

22 Article 4(1) of the GDPR in relation to the definition of personal data: "«personal data»: any information relating to an identified or identifiable natural person («data subject»)".

23 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free movement of non-personal data in the European Union.

24 Interesting is the Italian rule provided for in Article 64 paragraph 2-quinquies of the CAD (Digital Administration Code approved by Legislative Decree 82/2005 subsequently amended and supplemented) which provides for the exemption of liability arising from the general obligation to monitor activities on one's own websites where access is provided with the SPID digital identity system. This is because in this case the users are identified with certainty and therefore the activities carried out on hosted sites are ascribable with certainty to identified users and in no case fall to the hosting provider.

25 Art. 3 GDPR.

26 This is what Article 832 of the Civil Code provides, in a definition that has remained substantially unchanged since its codification.

27 In fact, according to Article 810 of the Civil Code, "goods are those things that can be the subject of rights".

28 An emblematic case, with reference to information, is for instance represented by the legal protection granted by the legal system to the so-called "Data Banks", defined by Article 2, no. 9 of Law 633/1941 as "collections of works, data or other independent elements systematically or methodically arranged and individually accessible by electronic means or otherwise", and deemed worthy of protection from third parties' abuse due to their economic value.

29 Pursuant to Article 1140 of the Civil Code, "possession is the power over a thing which is manifested in an activity corresponding to the exercise of property or of another right in rem. It may be possessed directly or by means of another person who has possession of the thing". As can be seen, the definition may perhaps be helpful in

reconstructing the "possession" of a bit by the various parties involved, but it does not help at all in defining whether those who possess such bits can or should be responsible for them upstream.

30 The term "control" is in fact the subject of many different regulatory definitions, all of which, however, are purely corporate in nature.

31 Without wishing to go into too much detail here about legal reconstructions, the etymology itself of the word leads one to consider the "title" of a right, i.e. the legally relevant act or fact, on the occurrence of which a person acquires the right (e.g.: as a general rule, pursuant to Article 2 of the Civil Code, a person acquires the capacity to act - and therefore to consciously carry out legally relevant transactions - as soon as he turns 18).

32 The legislative decree 115/2008 and subsequent amendments, which defines electricity grids and simple systems for the production and consumption of energy, speaks on several occasions of "ownership" of electricity production and consumption units by several legal entities.

33 First and foremost, the rules set out in Legislative Decree 70/2003 ad subsequent amendments, implementation of Directive 2000/31/EC on e-commerce.

34 This legal status is supported by the numerous Italian and international regulations on derivative works, which protect the creator of the works, without forgetting - at least on a moral level if not on a substantive level - the rights of the original works from which they derive.

35 Emblematic on this point is the wording of Art. 1677 of the Civil Code, according to which "if the purpose of the contract is the provision of continuous or periodic services, the rules of this chapter [editor's note: i.e. those of the contract] and those relating to the supply contract shall be observed in so far as they are compatible".

36 While, for instance, the SaaS cloud system provider offers software application services and will presumably have to guarantee their proper functioning, an IaaS cloud provider will, on the other hand, at least have the different obligation to make only virtualized hardware resources available to its customers.

37 The notion of Data Processor, originally referring to persons and entities that process personal data on behalf of the Controller and that may or may not also be present within the Controller's organization itself, has been modified following Opinion 1/2010 - WP 169 of the Art. 29 Working Party on the concepts of "controller" and "processor" (https://www.garanteprivacy.it/documents/10160/10704/wp169+-+Opinion+1+2010+on+the+concepts+of+ controller+and+incumbent+processors.pdf/64cd4700-f0d4-4-c04-b834-9c3da69a93ea?version=1.1), the concepts of which were then transposed into the GDPR. To date, the notion of Data Processor, defined in Art. 4(1)(8) of the GDPR as "the natural or legal person, public authority, service or other body that processes personal data on behalf of the controller", expressly regulates - together with Art. 28 GDPR - the role of a subject exclusively external to the controller's organization.

38 It should be pointed out at the outset that, although the GDPR expressly refers to specific types of data (which will be discussed shortly), it provides a general framework appropriate for use for a much wider range of generic "data".

39 This arrangement, provided for by the interaction between Articles 24 and 28 of the GDPR, is actually outlined by the same definitions of the two subjects, nn.7) and 8) of Art. 3 GDPR, and is codified as "accountability"; it translates into a greater burden of responsibility on the Owner, who determines means and methods of processing at his full

risk and responsibility), but who can then pour specific responsibilities on the external manager to whom he entrusts the data, and on whom he can then rely on a contractual level, in case of non-compliance.

40 Pursuant to Article 28(3) of the GDPR, "processing operations by a controller shall be governed by a contract or other legal act in accordance with Union or Member State law, binding the controller to the data controller and stipulating the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and the rights of the controller." This specific act, the specific contents of which are further regulated in the continuation of the paragraph in question, often takes the form of a Data Processing Agreement, often in conjunction with the clauses and provisions required for non-EU processing, in accordance with Articles 44-49 of the GDPR on the subject.

41 The prohibition in question is derived from Article 45 of the GDPR.

42 See Article 46(2) and (3) GDPR.

43 The provision is specifically designed to protect the right of data subjects to ensure that their personal data are not subjected to processing that is particularly "invasive" of their personal sphere, as it is likely to have a significant impact on it.

44 See for example https://www.corrierecomunicazioni.it/digital-economy/blackout-mondiale-per-google-services-tutto-risolto-in-poche-ore/;https://st.ilsole24ore.com/art/tecnologie/2011-04-29/incendio-server-arubait-tilt-121947.shtml?refresh_ce=1; https://www.bbc.com/news/technology-36460328.

45 See https://www.hostingtalk.it/cloud-computing-quando-il-provider-fallisce_-c0000067g/.

46 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

47 See for example the EBA Guidelines on outsourcing to cloud providers, which are binding for the financial and insurance industry: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers.

48 The plurality of orientations also derives from the different possible contents of the SaaS cloud contract: the data processing entrusted to the cloud software may in fact have different purposes and different contractual relevance, thus changing the applicable contractual type and the responsibility of the cloud provider. One thing is the monthly processing of salaries or the keeping of company accounts, another is the cloud-based use of an online video game.

49 Pursuant to Art. 1575 of the Civil Code, the landlord has three fundamental obligations: "1) to deliver the leased property in a good state of repair; 2) to keep the property in a state to serve the agreed use; 3) to guarantee to the tenant, during the tenancy, the peaceful enjoyment of the property". To these obligations must be added those set out in articles 1576-1577 concerning the maintenance of the leased property and its repairs, which assign to the landlord the activities of extraordinary administration, leaving to the tenant the ordinary ones.

50 Articles 1578-1581 of the Civil Code, according to which the landlord is liable for defects in the leased property (whether existing or occurring) and must compensate the tenant if he does not prove that he was unaware of such defects without fault at the time of delivery.

51 First, the obligation to receive the goods (the data) and to keep them with the dili-

gence of a good father, according to the provisions of Articles 1766 et seq. of the Civil Code.

52 Interesting in this respect is Google's "Transparency Report" available at URL https://transparencyreport.google.com/?hl=it and dealing with "Sharing of data that reveal how government and company regulations and actions affect data privacy and security, as well as access to data": within this report, at URL https://transparencyreport.google.com/user-data/overview?hl=it there is a special section listing data on global user information requests received by Google. In particular, with regard to Italy, we read that in the period July 2019-December 2019, out of 1486 requests relating to 2099 accounts, Google fulfilled, in whole or in part, about 50 per cent of them.

53 The best way would be to declare expressly applicable (in a contract subject to Italian law) both the rules of Art. 1560 et seq. of the Civil Code and, for all other aspects, the rules of Art. 1766 et seq. of the Civil Code.

54 Regardless of the "strength" and inviolability of the encryption. The fact that they are encrypted constitutes a logical barrier, like a door that is locked but which could be broken down with a light push: the fact that the door has to be "broken down" forces the cloud provider to take illegal action, which makes any obtaining of the data illegal.

55 A recent case that has caused a lot of uproar is the Amazon-AWS/Parler case, in which the American cloud provider interrupted the IaaS service of Parler, the favorite social platform of the American right-wing Trump supporters, effectively shutting it down. According to Amazon-AWS, Parler had violated the AUP due to false or dangerous content disseminated by users, thus necessitating the measure. Parler filed a lawsuit against Amazon-AWS (see: https://www.bbc.com/news/technology-55615214) on the grounds that he did not violate the AUP.

56 In the US Department of Justice's case against the cyberlocker Megaupload, which alleged the primary use of the service for sharing copyright infringing content, the service was shut down and the servers seized. Nonetheless, the question of whether (and how) data could be deleted, the storage cost of which was estimated at USD 9,000 per day, was a complex one. In fact, a theoretical interest of the users in recovering the data was recognized, even though the terms of use of the service warned users that storage entailed the risk of complete loss of the data at any time. Finally, the data were placed under the protection of the EFF (Electronic Frontiers Foundation) as a neutral body in charge of handling the remaining requests from users, to be carried out within a maximum time limit.

57 Such liability was alleged in the above-mentioned US case of the cyberlocker Megaupload on the basis that the cloud service in question had been designed and marketed for primary use in violation of the law. The case, however, never reached a substantive discussion, as termination of the service and criminal prosecutions took place before that. In the EU, the new Copyright Directive 2019/790 excludes "business-to-business cloud services" and "cloud services that allow users to upload content for personal use" from the special liability for content uploaded by users that it outlines: it ascribes the new liability regime to entities defined as "providers of online content sharing services", namely those whose main purpose or one of the main purposes is to store and give access to the public to large amounts of copyrighted works or other protected material uploaded by its users, which the service organizes and promotes for profit.

58 See Commission Explanatory Note https://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf.

59 See https://rm.coe.int/16802f423d.

60 As pointed out above (§ 1.3), information, already consisting of bits that can be disaggregated with the striping technique, can be distributed on various servers located in different jurisdictions, even simultaneously.

61 By "comity analysis" US law means - in extreme synthesis and greatly simplifying the subject - a procedure in which the judge considers the law of a foreign state "as a courtesy". The final decision, however, remains with the US judge who is not legally bound by the foreign provisions.

62 From this point of view, there have been no changes to the provisions of the SCA, which are confirmed and, therefore, US corporations, US domiciled corporations and corporations owned by US persons can be considered as "subject to US jurisdiction" for this purpose; however, also those corporations which do not fall within the above categories, but which nevertheless have significant contacts with the US (e.g., corporations conducting a significant activity in the US) may well be considered as subject to US jurisdiction such as to make the court consider the extension of jurisdiction possible. In these terms, the criteria for defining the subjects included or that may be included are not clear-cut, but are left to a case-by-case assessment by the judge; discretionary margins are also found in the assessment of the relationships between a company and its subsidiary in terms of control of the data owned or controlled by the latter by the former. It should be noted that, in such cases, the structure and relationship between the two companies does not affect the assessment, which must in any event be carried out by the court. At the outcome of this assessment, it will be decided whether or not the warrant can be issued.

63 See above, § 2.1.

64 This is a certification, to be carried out in advance, by the US Attorney General of Congress.

65 See Agreement of 3 October 2019 between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, available online at https://cli.re/jJ7Z3D.

66 See https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html.

67 See Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses done at Amsterdam; 2 June 2016, available online at:

68 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.

69 See Schwarz-Peifer, Data Localization, Under the CLOUD Act and the GDPR, Computer Law Review International, 2019/1.

70 See White Paper Google on Data residency, operational transparency,and privacy for European customers on Google Cloud, available online at: https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf?hl=cs.

71 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, nn. 27 e 28 available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN.

72 See the joint EDPB/EDPS response of 12 July 2019, accessible at the following link: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_de in which the EPDB concluded that: "service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the US on such requests.".

73 https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf See the position paper of 28 February 2019 accessible at the following link: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf.

74 Act of 5 February 2019, accessible at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0070.

75 Proposal of 17 April 2018 accessible at the following link: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

76 See European Commission Communication of 2 July 2014 "Towards a thriving data-driven economy", as well as Communications of 25 April 2018 and 15 May 2018.

77 Article 3, nr. 5, defines an obligation to locate data as "any obligation, prohibition, condition, limitation or other requirement, provided for by the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practice in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which requires the processing of data to be carried out on the territory of a particular Member State or which impedes the processing of data in another Member State".

78 Defined by the Regulation as "an authority of a Member State or any other body authorized under national law to exercise a public function or to exercise public authority, which is entitled to obtain access to data processed by a natural or legal person for the purpose of carrying out its official functions, as provided for by Union or national law". As we can see, the definition leaves the door open to the fact that the Authority can also be a foreign body, provided it is "authorized".

79 See for example the Parler / AWS Amazon case, already cited.

THE REACHABILITY OF DATA: A LEGAL PERSPECTIVE

This research work was
promoted and sponsored by:

DHH S.p.A.
(Milan Stock Exchange AIM DHH.MI - http://dhh.international)

Publication date:
December 2020

THE REACHABILITY OF DATA: A LEGAL PERSPECTIVE

Research by:
Innocenzo Genna
Eugenio Prosperetti

With the collaboration of:
Giulio Pascali
Davide Tuzzolino

sponsored by DOMINION HOSTING HOLDING

Publication Date
December 2020