universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„European Privacy and Data Protection in Cloud Computing in the Light of the Legal Practice in Spain: A Comparative Analysis“

verfasst von / submitted by

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Univ. Prof. Dr. Dr. hc. Peter Fischer

I would like to begin by thanking my supervisor, Prof. Dr. Peter Fischer, for accepting my topic and let me work on something I am passionate about. Of course to my parents, that have always being my biggest support and let me experience new paths in my life. And to Nils, thank you for your help and being along the way.

TABLE OF CONTENT

LIST OF ABREVIATIONS

AEPD: Spanish Data Protection Agency
CJEU: Court of Justice of the European Union
DPD: Data Protection Directive
ECP: European Cloud Partnership
EDPB European Data Protection Board
EDPS: European Data Protection Supervisor
EEA: European Economic Area
ENISA: European Union Agency for Network and Information Security
EU: European Union
FP7: Framework Programme 7
GDPR: General Data Protection Regulation
ICT: Information And Communication Technology
IP: Internet Protocols
IT: Information Technology
ITL: Information Technology Laboratory
LOPD: Spanish Organic Law 3/2018, for the Protection of Personal Data and for the granting of digital rights
NIF: National Interoperability Framework
NIST: National Institute Of Standards And Technology
OECD: Organisation for Economic Co-operation and Development
OECD Guidelines: Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
OWASP: The Open Web Application Security Project
SME: Small And Medium-Sized Enterprises
TESTA: Trans European Services For Telematics Between Administrations
TFEU: Treaty on the Functioning of the European Union

‘‘Cloud’ is no longer a mere buzzword for cool technology, but rather represents a significant paradigm shift in technological advancement and our daily lives.’

- Anne S.Y. Cheung and Rolf H. Weber.

‘I don’t need a hard disk in my computer if I can get to the server faster… carrying around these non-connected computers is byzantine by comparison.’

- Steve Jobs.

‘Do not be confused. Clouds are not a data protection free zone.’

- Stewart Dresner, Chief Executive, Privacy Laws & Business.

INTRODUCTION

Significance of cloud computing

As technological revolution continues to evolve, cloud computing has become an essential part of our lives. In this regard, George Reese, writer in the field of cloud computing, has stated that 'whilst the Internet is a necessary basis, the cloud is something more important. It is a place where technology is used when it is necessary, and whilst it is necessary, not a minute more'.

But the truth is that any technological development posses new challenges. Far from understanding the tremendous implications for individual's life, the huge increased of global data flow has brought big concerns for the security of individual's personal data. In other words, processing personal data raises general fears that have been taken into account and will be tackle in the future by the European institutions and legal bodies. The European Competition Commissioner Margrethe Verstager, at Globsec 2018 in Slovakia, agreed that in regard to the future of data and competition 'We have to look dangerous'.

But is the current regulatory framework enough to deal with the issues intrinsic to cloud computing, while still allowing the growth of technological innovation for the European Union? Along this paper, it will be presented the most relevant legal issues when engaging cloud services, by taking the General Data Protection Regulation and the different policy guidelines provided by the EU institutions into consideration, as well as the Spanish public administration guidelines and instrument issued over the last years.

Cloud computer represents itself as one of the most important technologies for the future of companies, public administrations and individuals. Thus it is inevitable that, the adoption of this new paradigm has become a priority. Nevertheless, new approaches will have to take into consideration the nature of 'the cloud' and the concerns for the privacy and data protection of the individual that are intrinsically linked to it. The reality is that cloud computing

represents an endlessly technology and its significance will not stop from growing. In an on-going technological revolution, it seems like we are just taking the first steps.

Chapters' overview

The opening Chapter focuses on the importance to establish a standard definition of cloud computing by providing the most agreed technical definition and presenting broadly what are the different cloud computing service models and which are the most relevant deployment models for 'the cloud'. To conclude with Chapter 1, it is shown briefly the importance and benefits of cloud computing, especially why the European institutions and the different public Administration are engaging in the use of cloud services.

Chapter 2 turn its attention to data protection due to the regulatory challenges posed by cloud computing. With special emphasis on the General Data Protection Regulation and the official policy documents provided throughout the last years by the European Commission and the different European bodies, it will be compared the Spanish regulatory framework by highlighting its particularities. While analysing the current legal basis on data protection, it will be presented possible vulnerable scenarios and difficulties in the legislation with regard to cloud computing.

Chapter 3 concludes by establishing the available regulatory policy documents for cloud computing within Spain, and the general framework in the European Union. As this Chapter will show, the cloud is without a question a very attractive business to engage by the public authorities. Prove of it, it is the different policy documents issued by the administration, both in Spain and at the European level.

Finally, and to conclude, there will be exposed an overview of the conclusions to the different Chapters, by giving a general perspective of the future of cloud computing and what are the challenges that shall may be faced in the following years in the European Union.

CHAPTER 1. THE FOUNDATION OF CLOUD COMPUTING

The way in which technology services are delivered has changed over the last years. Together with the evolution of Internet, cloud computing is one of the services that have led to this transformation. However, the technology behind cloud computing is constantly evolving, what it makes difficult to catch all the aspects of it into one definition.[1] In the same vein, its use has generated in many challenges and legal issues; and although the legal approach is essential, in the first place, Chapter 1 turns its attention to give a standard definition of cloud computing from a technological perspective.

1.1. CONCEPT OF CLOUD COMPUTING

Knowledge of cloud computing have a great importance for international organizations that deal specifically with standardizing information technology[2] (hereinafter referred to IT).[3] The most agreed definition used by different research papers in the matter is the one provided by the National Institute of Standards and Technology (hereinafter referred to as NIST)[4], which together with the Information Technology Laboratory (hereinafter referred to as ITL)[5], have provided an authoritative guideline[6] to cloud computing:

[1] B.J.A. Schellekens, 'The European Data Protection Reform in the Light of Cloud Computing' (Master Thesis, University of Tilburg 2013)

[2] IT is the use of computers to store, retrieve, transmit, and manipulate data, or information, normally in the context of a business. Products or services within an economy are associated with information technology, including computer hardware, software, electronics, semiconductors, internet, telecom equipment, and e-commerce, see definition of IT provided in <https://en.wikipedia.org/wiki/Information_technology#cite_note-2>

[3] Luis Joyanes Aguilar, 'Cloud Computing Notes for a Spanish Cloud Computing Strategy' (2012) Journal of the Higher School of National Defence Studies 83, 103

[4] NIST was founded in 1901 and is now part of the U.S. Department of Commerce. It is one of the nation's oldest physical science laboratories. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations, see About NIST (*NIST* 2018) <https://www.nist.gov/about-nist>

[5] ITL at the NIST promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure, see Peter Mell, Timothy Grance, 'The NIST Definition of Cloud Computing' (*National Institute of Standards and Technology Information Technology Laboratory,* 2011) Special Publication 800-145

[6] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM (2012) 529 final Unleashing the Potential of Cloud Computing in Europe [2012]

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models". [7]

The European Commission (hereinafter referred to the Commission) has defined it as an Internet-based computing whereby, software, shared resources and information are on remote servers ('in the cloud')[8]. The Commission refers to the idea that throughout 'the cloud' any information can be easily accessible anywhere in the world to anyone who has access to Internet. Thus, 'the cloud' turns into a new service for the processing of information. Together with the Commission's definition, the European Union Agency for Network and Information Security[9] (hereinafter referred to ENISA) characterised cloud computing as a new way of delivering computing resources, not a new technology.[10] Consequently, cloud computing as a service takes shape of an IT product made from cloud computing technology.[11]

To provide these services, there are big companies specialized on it, which put at the disposal of the users the infrastructure[12] or software. As an illustration, "[t]he cloud can be infra-

[7] Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing' (*National Institute of Standards and Technology Information Technology Laboratory,* 2011) Special Publication 800-145

[8] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM(2010) 609 final A comprehensive approach on personal data protection in the European Union [2010]

[9] ENISA is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors, see ENISA, 'Cloud Computing. Benefits, risks and recommendations for information security' (2009)

[10] ENISA, 'Cloud Computing. Benefits, risks and recommendations for information security' (2009) 4

[11] Cholada Ratanachuesakul, 'The Legal Status of a Controller and a Processor of a Cloud Service Provider Under the GDPR in the Context of the Complete Protection to the Data Subject' (Thesis, Tilburg Institute for Law, Technology and Society (TILT) LL.M. Law and Technology, 2017-2018) 12

[12] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer, see Mell and other (n 7) 2

structure or software. In other words, it can be either an application accessed from the desktop and run immediately after downloading, or it can be a server that is invoked as necessary. In practice, cloud computing provides either a software or hardware service."[13]

The main stakeholders in the world of the cloud are generally two: on one hand, the cloud provider or supplier, providing the technology, infrastructure and information; and on the other hand, the 'end user', who will be the one having access and using the cloud services.[14] The leading cloud service providers are VMware, Sun Microsystems, Rackspace US, IBM, Amazon, Google, BMC, Microsoft, Ubuntu and Yahoo. These big companies make use of virtual machines, which are designed through 'software implementations of computers used to execute programmes'.[15]

1.1.1. Essential Characteristics

There are few key features to highlight from the prior definition of cloud computing: (1) on-demand self-service; (2) broad network access; (3) resource pooling; (4) rapid elasticity; and (5) measured service.[16]

On-demand self-service: 'A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider'.[17] This way, the user has unilateral access to the cloud services whenever required.[18]

Broad network access: 'Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g.,

[13] Joyanes (n 3) 86
[14] Joyanes (n 3) 87
[15] Joe Kong, Xiaoxi Fan and K.P. Chow, 'Introduction to cloud computing and security issues' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016)
[16] Mell and other (n 7) 2
[17] Ibid
[18] Joe Kong and others (n 15) 13

mobile phones, tablets, laptops, and workstations)'.[19] The cloud service is location independent enabling the users to use it 'through the cloud'.[20]

Resource pooling: 'The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth'.[21] There exists the effective use of resource sharing between different users all around the world.[22]

Rapid elasticity: 'Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time'.[23]

Measured services: 'Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service'.[24]

[19] Mell and other (n 7) 2
[20] Joe Kong and others (n 15) 13
[21] Mell and other (n 7) 2
[22] Joe Kong and others (n 15) 13
[23] Mell and other (n 7) 2
[24] Ibid

This being said, cloud services can also be distinguished from one to another, according to the model of services they provide and to the deployment models or structures used[25] for different cloud services.

1.1.2. Service Models

Cloud computing can be considered as a group of IT services, which should be defined and available to choose from.[26] There are three service models applying to issues regarding the cloud: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

SaaS: 'The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.[27] The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings'.[28] This service provides with the infrastructure and platforms, but also with the application software. Security and privacy provisions rely mainly on the cloud provider. Examples of cloud providers of SaaS are Facebook, Google Maps and YouTube.[29]

PaaS: 'The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the

[25] Ratanachuesakul (n 11) 12
[26] Joe Kong and others (n 15) 13-14
[27] See definition of cloud infrastructure (n 12).
[28] Mell and other (n 7) 2
[29] Joe Kong and others (n 15) 15

application-hosting environment'.[30] This service provides with the platforms and tools, so that the users can construct, install and develop their own applications. Security and privacy provisions are divided between the provider and the user. Cloud providers of PaaS are Google's App Engine and Microsoft's Windows Azure.[31]

IaaS: 'The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of selected networking components (e.g., host firewalls)'.[32] These kinds of providers are normally specialized on the cloud market and can rely on a physical and more complex infrastructure.[33] Security and privacy provisions far from the basic infrastructure rely on the users. Cloud providers of IaaS are Rackspace and Amazon EC2 and S3.[34]

The three service models can work as integrated or multi-layered service as well. This is the case of the famous platform Dropbox. As cloud provider, Dropbox works for the users as a SaaS supplier of the infrastructure, platform and software; however, Dropbox itself uses Amazon's IaaS infrastructure.[35]

1.1.3. Deployment Models

Besides the different types of service models, cloud computing can be classify according to implementation models or 'deployment models' for the cloud infrastructure. There are main-

[30] Mell and other (n 7) 2-3
[31] Joe Kong and others (n 15) 14
[32] Mell and other (n 7) 3
[33] Article 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' (WP 196, 1 July 2012)
[34] Joe Kong and others (n 15) 14
[35] Ibid 15

ly four deployment models: private cloud, community cloud, public cloud, and hybrid cloud. The deployment model refers to the system of 'resource sharing'.[36]

Private cloud. 'The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises'.[37]

Community cloud. 'The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises'.[38]

Public cloud. 'The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider'.[39]

Hybrid cloud: 'The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)'.[40]

Security and privacy provisions for the different deployment models vary on the effectiveness of the relevant policies, the strength of the security and privacy controls, and the scope of the transparency of the performance and management details of the cloud infrastructure.

[36] Joe Kong and others (n 15) 15
[37] Mell and other (n 7) 3
[38] Ibid
[39] Ibid
[40] Mell and other (n 7) 3

Amid all the deployment models, the private cloud offers the highest degree of control to the user, while the public cloud offers the lowest.[41]

All in all, it is likely that new mechanisms, functions and applications will be added to actual cloud computing service in the following years, which can lead to changes on the fundamental design and usage of cloud computing[42] provided along this Chapter and paper.

1.2. THE CLOUD BUSINESS MODEL

Over the last years, the cloud has made accessible information anywhere to anyone with access to Internet.[43] But one of the facts that better explains its success is its link to business, in particular, the benefits that bring to companies and public administrations, among many other stakeholders. Previously explained, the different cloud service models allow businesses to use central processing units cycle without having to buy the software themselves.[44] Likewise, users of the cloud enjoy the benefits of sharing their data anytime, anywhere, from any device and with anyone, all this at very low cost and high efficiency too.

The idea of relying on remote services providers for storing and computing needs seems more appealing more and more. This is one of the reasons why big large information and communication technology companies (hereinafter referred to as the ICT) have introduced strategies into their business willing to develop cloud computing. The leading firm Gartner[45] estimates that by 2020, a corporate "no-cloud" policy will be as rare as a "no-internet" policy is today.[46] Following Gartner predictions, 'by 2019, more than 30 per cent of the 100 largest vendors' new software investments will have shifted from cloud-first to cloud only'

[41] Joe Kong and others (n 15) 15
[42] Takato Natsui, 'Cloud Computing Service and Legal Issues' Meiji University, Tokyo, Japan 3
[43] Joe Kong and others (n 15) 8
[44] Ibid 9
[45] Gartner, Inc., is the world's leading research and advisory company, by equipping business leaders with insights, advice and tools to build the successful organizations of tomorrow, see About Gartner in < https://www.gartner.com/en/about>
[46] Amy Ann Forni and Rob van der Meulen, 'Gartner Says By 2010, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today' *Gartner* (Stamford, Conn., June 22 2016)

and ‘by 2020, more computer power will have been sold by IaaS and PaaS cloud providers than sold and deployed into enterprise data centres’.[47]

In the light of its significance, the European Union (hereinafter referred to EU) has adopted numerous policies towards the adoption of cloud computing. Back in 2011, the Vice-President of the European Commission for Digital Agenda, Neelie Kroes, spoke for the necessity of moving towards being ‘cloud-active’ and not just ‘cloud-friendly’.[48] In more detail, Chapter 3 develops the different approaches and current policy on cloud computing set up within the Digital Single Market Strategy for Europe.

To conclude, it should remain that the positive effects of cloud computing also raise big challenges not seen before, especially in data protection and user privacy. The Open Web Application Security Project (hereinafter referred to OWASP) referred to personal data protection as one of the ten issues for cloud computing.[49] This topic will be discussed along Chapter 2.

[47] Forni and other (n 46)
[48] Neelie Kroes, ‘Towards a European Cloud Computing Strategy’, speech delivered at World Economic Forum Davos (European Union, 27 January 2011); and Joe Kong and others (n 15) 10
[49] Ibid

CHAPTER 2. DATA PROTECTION

2.1. THE CLOUD COMPUTING SERVICE

As can be imagined at this early point, cloud computing may reach a wide range of fields. But in spite of its complex nature or the multiple benefits that come with it, the issues of data protection only set to increase in importance when analysing cloud computing. Unlike traditional computing methods in which the owner of the information is responsible for their own data[50], cloud computing relies on online resources. Consequently, this situation can lead to various scenarios. In most cases, the users and the providers by putting personal data on remote servers can end up losing control over it for numerous reasons. Intrinsically, cloud computing, which acts storing a vast amount of data, becomes a valuable target of unauthorized access or misappropriation. Chapter 2 will favour an important approach to data protection within the cloud computing service, with a special emphasis in the regulation on data protection within the European Union and Spain.

2.2. REGULATORY FRAMEWORK

Since 1973, more than 100 jurisdictions[51] have promulgated data protection laws following mostly the principles gathered in the 'Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (hereinafter referred to OECD Guidelines), provided by the Organisation for Economic Co-operation and Development (hereinafter referred to OECD).

2.2.1. General Data Protection Principles

[50] Ratanachuesakul (n 11) 17
[51] Graham Greenleaf, 'Global Data Privacy Laws 2013: 99 Countries and Counting' (2013), 123 Privacy Laws and Business International Report 10

These core principles, applicable and relevant to 'the cloud'[52] as well, were updated in 2013 and are as follows:[53] Collection Limitation Principle; Purpose Specification Principle; Use Limitation Principle; Data Quality Principle; Security Safeguards Principle; Openness Principle; Individual Participation Principle; Accountability Principle; and Principle of Free Flow and Legitimate Restrictions.[54] When engaging cloud services, data users must observe all of the data protection principles:[55]

The Collection Limitation Principle normally applies to data collected for business purposes and the collection should be 'purpose-driven'. Besides this, the means of the collection should be lawful and fair, and where applicable, the data users should notify the data subjects the purpose of data collection and obtain their consent.

The Purpose Specification Principle means that the purpose for the collection of data should be specified 'no later than at the time of collection'. When the collection has expired its purpose, the data must be erased or anonymized (if practicable). When engaging cloud services, cloud providers must ensure that personal data is intended to be erasing, when it no longer serves a purpose.

The Use Limitation Principle recognizes that personal data entrusted to cloud providers may not be used for purposes beyond those collected and/or agree upon on (except with the consent of the data subject).

The Data Quality Principle establish that the collection of personal data must be pertinent to the purpose for which it has been collected, therefore, it has to be accurate, complete and keep up to date.

[52] Henry Chang, 'Data Protection regulation and cloud computing' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016) 29-30
[53] OECD, 'The OECD Privacy Framework' (2013) 11-17
[54] The principles are selected from Chapter 1 and Chapter 2 of the OECD Privacy Guidelines (n 53)
[55] Chang (n 52) 29-32

The Security Safeguards Principle, as logic as it may sound, recognizes that efficient security safeguards from loss, unauthorized access or use, destruction, modification or disclosure must protect personal data.

The Openness Principle, sets that any developments, practices and policies that deal with handling personal data must be known and accessible.

The Individual Participation Principle establish that any individual whose data has been collected on the right to confirm whether its data has been held by a data user, to obtain a copy of such data (within a reasonable period of time), and to have the data erased, rectified, completed or amended (as appropriate). This means that data users must ensure that cloud providers are able to support data users' obligations concerning the fulfilment of data access and data correcting request.

The Accountability Principle determines that, when engaging cloud services, data users should assess all privacy impacts, the so-called privacy impact assessment. Data users also should ensure that cloud providers are able to provide appropriate incident responses and breach handling procedures.

The Principle of Free Flow and Legitimate Restrictions recognizes that own jurisdictions may restrict the transfer of personal data when the other jurisdiction cannot provide the former data protection principles.

2.2.2. Current Data Protection Legislation In The EU

In the EU, Member States have enacted their data protection laws following the principles set forth by the Directive 96/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data

and on the free movement of such data[56] (hereinafter referred to DPD). However, on 25 May 2018, the entry into force of the General Data Protection Regulation[57] (hereinafter referred to GDPR), has suspended the DPD. In hopes of 'a better achieving cross-EU harmonization', the GDPR was enacted in the form of a regulation, which no requires any national implementing legislation and became law directly in all Member States.[58] With the current GDPR in force, the European regulation on data protection is seemed as one of the most exigent in the world.

2.2.3. Current Data Protection Legislation In Spain

In like manner, Spain has been recognized as one of the four most rigorous countries in the world concerning data protection legislation.[59] The Spanish Constitution of 1978[60] protects data protection as a fundamental right derived from respect for the dignity of human beings. Thus, section 18 paragraph 4 of the constitutional text assures that 'the law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights'.[61] Although protected by the constitutional text, data protection is not an absolute right and, where applicable, must be weighing with other fundamental rights, as well as other legitimate interests.[62]

---

[56] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)

[57] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[58] W. Kuan Hon, 'Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens' (2017), Edward Elgar Publishing, 12-13

[59] Meghan Kelly, 'These 5 countries were ranked best for privacy (infographic)' *Venture Beat* (13 October, 2013) in https://venturebeat.com/2013/10/13/countries-privacy/

[60] Spanish Constitution of 1978 (as amended on August 28, 1992)

[61] Ibid

[62] Reyes Bermejo Bosch and Leticia López-Lapuente, 'The Privacy, Data Protection and Cybersecurity Law Review' [2017] The Law Reviews, The Privacy, Data Protection and Cybersecurity Law Review - Edition 4 in < https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151343/spain>,>

In the same line, the GDPR points out that 'the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 (1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16 (1) of the Treaty on the Functioning of the European Union (hereinafter referred to TFEU) provide that everyone[63] has the right to the protection of personal data concerning him or her'[64] and, furthermore, 'it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality'.

Thus, Article 18 of the Spanish Constitution lay the foundation for the legal and institutional framework for the protection of personal data, which was developed by the following legislation: the Organic Law 5/1992, of 29 October, of the Automated treatment of Data; the Organic Law 15/1999, of 13 December, of Data Protection; the Royal Decree 994/1999, of 11 June, that approved the Regulation on Security Measures for automated files that contain personal data; and the Regulation of Development, Royal Decree 1720/2007, of 21 December, which approved the Regulation implementing the Organic Law 15/1999.[65]

However, and very recently on time, on 21 November 2018, the Spanish Parliament approved in compliance with the GDPR[66], the new 'Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales'[67] (hereinafter referred to LOPD), or in English, the 'Spanish Organic Law 3/2018, for the Protection of Personal Data and for the granting of

[63] 'The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data', see General Data Protection Regulation (n 57) Recital (2)
[64] General Data Protection Regulation (n 57) Recital (1)
[65] Cristina Pauner and Jorge Viguri, 'The Adaptation Of The GDPR In Spain: The New Data Protection Act (LOPD)' (2018), E-conférence, National Adaptations of the GDPR
[66] With regard to other Member States in the EU, the German government has passed the 'Act to adapt Data Protection Law to Regulation (EU) 2016/679 and to implement Directive (EU) 2016/680 on June 30th, 2017. In Austria, on July 31st, 2017, it was enacted the 'Data Protection Amendment Act 2018'. In Belgium, on December 3th, 2017, the government passed its own implementation in compliance with the GDPR 'Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnet'. In Slovakia, on November 29th, 2017, it was adopted the Bill that annulment the Act on Data Protection n. 122/2013 and implements the GDPR from May 25th, 2018. In Italy, it was enacted the law to reform the 'Codice in material di protezione dei dati personali', see Pauner and other (n 65) 1
[67] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE-A-2018-16673)

digital rights'. Coinciding with the 40th anniversary of the Spanish Constitution, as from 7 December 2018, the new Data Protection Act has entree into force, superseding the former Spanish data protection legislation and provisions that contradict, oppose or are incompatible with the GDPR.

- **Spanish Data Protection Act (LOPD)**

Amidst numerous rumours for early called elections, and after many months of tensions, the Spanish Parliament approved the new LOPD, after being nearly two years in development.[68] The new legal text is conformed of ninety-seven articles organized in ten titles, twenty-two additional provisions, six transitional provisions, one repealing provision and sixteen final provisions. Furthermore, it grants a set of rules associated with the Internet environment, the so-called 'digital rights', by undertaking the responsibility of recognising and safeguarding them to every individual. The particularities of the LOPD compared to the GDPR fall on, for instance, in the age underage individuals need to have to grant consent for the processing of their data, the possibility to offer information by means of a layered system, or the specific circumstances in which a data protection officer needs to be appointed.[69]

But the new data protection act has already been criticised, even if the text was approved with 220 votes in favour and 21 against[70] in the parliament. Critics have stated that the new law does not fully comply with the collection of data regarding people's political opinions in regard to the GDPR. The European regulation establishes that processing 'of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, (…) shall be prohibited'.[71]

---

[68] Paloma Bru and Paula Fernández.Longoria, 'Spain finalises new data protection and digital rights law' *Out-Law.com* (27 November 2018) in https://www.out-law.com/en/articles/2018/november/spain-new-data-protection-digital-rights-law/

[69] Guadalupe Sampedro and Ester Vidal, 'A new Data Protection Act for Spain' *Bird & Bird* (December 2018) in < https://www.twobirds.com/en/news/articles/2018/spain/new-data-protection-act-for-spain>

[70] 'Spain approves contested data protection law', *Mail & Guardian* (22 November 2018) in < https://mg.co.za/article/2018-11-22-spain-approves-contested-data-protection-law>

[71] 'Paragraph 1 shall not apply if one of the following applies: (…) (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body

However, the striking provision in the LOPD sets out in Article 58 *bis*, called the 'Use of technological means and personal data in electoral activities', that '[t]he collection of personal data related to political opinions of individuals carried out by political parties in the framework of their electoral activities will be protected by the public interest only where adequate guarantees are offered'. Proceed with 'political parties, coalitions and electoral groups may use personal data obtained in web pages and other public access sources for carrying out political activities during the electoral period'.[72]

Spanish consumers group, FACUA, and some far-left parties such as 'Unidos Podemos', in separate statements, have already claimed that they will challenge such premise before the Spanish Constitutional Court[73], due to its unconstitutional nature. It is only a matter of time before they deliver as promised and we could know what is the opinion of the Constitutional court. Certainly, the question also remains whether the article will be interpreted by the Spanish Data Protection Agency either according purely to the LOPD or in a broader sense. Nevertheless, the Spanish authority has already set its opinion in the matter[74], knowing in advance of the problems that could arise in the near future regarding the application of such article.

- **Spanish Data Protection Authority**

---

with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects', see General Data Protection Regulation (n 57) Article 9 paragraph 1 and paragraph 2

[72] Miquel Peguera, 'New Spanish Law Raises Concerns Over Use Of Sensitive Data By Political Parties', (Stanford Law School, The Center for Internet and Society, 24 November 2018) in < https://cyberlaw.stanford.edu/blog/2018/11/new-spanish-law-raises-concerns-over-use-sensitive-data-political-parties>

[73] Mail and Guardian (n 70)

[74] Agencia Española de Protección de Datos, 'Criterio de la Agencia Española de Protección de Datos sobre cuestiones electorales en el proyecto de nueva LOPD', (2018) in https://www.aepd.es/prensa/2018-11-21.html

'La Agencia Española de Protección de Datos', that is to say, the Spanish Data Protection Agency[75] (hereinafter referred to AEPD) has contributed in the last months (up to this date, January 2019) to the satisfactory implementation of the GDPR through different guiding principles and basic guidelines.[76] The AEPD was created in 1993, and it has been active in its role of educating organisations and the general public on the value of data protection and of imposing significant sanctions.

On 11 June 2018, the AEPD published its Memorandum of 2017. In 2017 alone, it received 10.651 claims from individuals and authorities. There has been a considerable increase (36.8%) in the last two years of the complaints filed with the Agency in relation to the processing of data on the Internet, which went from 557 in 2015 to 762 in 2017.[77] Now that the GDPR is in force since May 2018, it also remains to be seen how the AEPD and Member States data protection authorities will continue disposing of their functions.

2.3. GENERAL DATA PROTECTION REGULATION (GDPR)

The following epigraph will be dedicated to the analysis of the most relevant aspects for 'the cloud' under the GDPR scope. As an integral part of the cloud computing framework, the GDPR guarantee that personal data –being data from which a person can be identified-, is granted extra protection and is not disclose to parties which not require and are not entitled to receive this information. However, it must not be forgotten that the application of the law to the context of cloud service is not enough and clear yet, especially in matters dealing with the role of the cloud service provider; since the diverse nature of cloud service providers

[75] DPAs offer expert advice on data protection issues, by informing the general public on the rights and obligations related to data protection and in particular the General Data Protection Regulation (GDPR)', see Commission, 'What is the role of the Data Protection Authority?' in https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority_en

[76] AEPD, 'Responsabilidad proactiva' in https://www.aepd.es/reglamento/cumplimiento/principio-responsabilidad-proactiva.html

[77] AEPD, 'La Agencia Española de Protección de Datos publica su memoria 2017' in < https://www.aepd.es/prensa/2018-06-11.html>

originate doubts when it comes to the protection of personal data stored in 'the cloud'. Furthermore, it must also be remember the diverse nature of the cloud service environment.

2.3.1. Definition Of Personal Data

The establishment of a definition of personal data is fundamental for the purpose of this Chapter. Due to a big reliance on cross-border hosting and outsourcing, cloud computing can lead to great uncertainty concerning the processing of data. This insight is further enhanced by the lack of a standard definition of what falls under the scope of 'personal data'. As a general criterion, acceptance relies on whether data can be linked to an identifiable or identified individual.[78] Yet it should remain that the definition may vary in the different jurisdictions around the world, and that technological development continues to create challenges to its interpretation nowadays.[79]

The current personal data's definition in the EU incorporates identified and identifiable notions of living individuals. The foundation of such definition was born back in the mid-1990s when the DPD[80] was first enacted and it was required to approach the interest to bring up by personal data transfers to countries outside of the EU.[81] Later on, the creation of 'Article 29 Working Party'[82], an advisory body on data protection in the EU, made possible the enactment of the Opinion 4/2007 on the concept of personal data.[83] The opinion[84] provided

[78] Anne S. Y. Cheung, 'Re-personalizing personal data in the cloud' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016) 69

[79] Dominic N. Staiger, 'Cross-border data flow in the cloud between the EU and the US' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016) 97

[80] Data Protection Directive 95/46/EC (n 56)

[81] Staiger (n 79) 96

[82] The Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC

[83] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (01248/07/EN WP 136)

[84] The Working Party issued numerous documents, which are relevant for the purpose of cloud computing, as such the Opinion 05/2014 on Anonymization Techniques onto the web; Opinion 03/2014 on Personal Data Breach Notifications; Opinion 03/2013 on Purpose Limitation; Opinion 15/2011 on Consent; Opinion 08/2010 on Applicable Law

with a better understanding of the concept of personal data and the situations in which national data protection legislation should be applied.[85] As of 25 May 2018, 'Article 29 Working Party' has been replaced by the European Data Protection Board[86] (hereinafter referred to EDPB), which it is now in charge of the application of the GDPR.

At the present time, article 4 (1) of the GDPR contains the legal definition of personal data. According to it: '"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[87]

The dimension of personal data's definition is such that only anonymous data[88] is not including in it.[89] This is due to anonymous data does not normally lead to the identification of an individual.[90] However, it should be taken into consideration that 'by merging an anonymous dataset together with another anonymous data set, an individual person can potentially

[85] Article 29 Data Protection Working Party (n 83)
[86] 'EDPB is the body in charge of the application of the General Data Protection Regulation (GDPR) as of 25 May 2018. It's made up of the head of each DPA and of the European Data Protection Supervisor (EDPS) or their representatives. The European Commission takes part in the meetings of the EDPB without voting rights. The secretariat of the EDPB is provided by the EDPS (…). The EDPB will help ensure that the data protection law is applied consistently across the EU and work to ensure effective cooperation amongst DPAs. The Board will not only issued guidelines on the interpretation of core concepts of the GDPR but also be called to rule binding decisions on disputes regarding cross-border processing, ensuring therefore a uniform application of EU rules to avoid the same case potentially being dealt with differently across various jurisdictions', see General Data Protection Regulation (n 57) Articles 63 to 76 and Recitals (135) to (140) and the definition provided by the Commission in https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en
[87] General Data Protection Regulation (n 57)
[88] 'The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes', see General Data Protection Regulation (n 57) Recital (26)
[89] Luigia Altieri and Gianmarco Cifaldi, 'Big data, privacy and information security in the European Union' (2018), Sociology and Social Work Review, 57
[90] Staiger (n 79) 97

be identified via a computerized calculating process such as is commonly used in Big Data[91] technology'.[92] The development of 're-identification technology'[93], has also led to data being 're-personalized'.

The problem stems from the huge development of cloud computing services. Due to the big amount of data stored in cloud systems, the using of patterns to identify living individuals has become much easier, and as a result, it has lowered 'the efforts required to identify and attribute specific characteristics to an individual.[94] Therefore, it would seem appropriate an agreement upon standards in regard to the identifiability of personal data, for the purpose of ensuring legal certainty, especially for cloud providers.

- **Legal Safeguards**

There are three main methods that could work to prevent the identification of personal data: encryption, pseudonymization or anonymization. 'When data is encrypted it is generally no longer classed as personal data because "if you cannot view data, you cannot identify data subjects"[95] […]. Nevertheless, such an assessment will strongly depend on the type of encryption used and the security level it provides.[96] Anonymized and pseudonymized data are altered through a one-way measure which cannot easily be reversed'.[97]

[91] '"Big Data" refers to the processing of vast amounts of data *in order* to determine correlations between data sets that provide valuable information for various commercial purposes', see definition of Big Data given in Staiger (n 79) 98
[92] Staiger (n 79) 98
[93] It is the process of matching anonymous data (or also known as 'de-identified data') with publicly available information, with the purpose of discovering the individual to which the data belongs to, see in https://en.wikipedia.org/wiki/Data_Re-Identification
[94] Staiger (n 79) 99
[95] W. Kuan Hon, Christopher Millard and Ian Walden, 'The problem of "Personal Data" in Cloud Computing' (2011) 1 IDPL 211-215
[96] W. Kuan Hon, Eleni Kosta, Christopher Millard and Dimitra Stefanatou, 'Cloud Accountability: The likely impact of the Proposed EU Data Protection Regulation' (2014) Queen Mary School of Law Legal Studies Research Paper 172/2014, 10-13
[97] Staiger (n 79) 98

In the same line, the GDPR recognizes the importance of implementing measures to lower the risks associated with the processing, such as encryption.[98] Therefore, either the controller or the processor, characters that will be explained consecutively, must assess possible risks and ensure an appropriate level of security.[99] Additionally, the GDPR also sets up the importance of the appliance of pseudonymization[100] as a way to reduce the risks associated when processing personal data.[101]

2.3.2. Definition Of Processing

Together with the definition of personal data, it is fundamental to establish a definition of processing. For the GDPR, '"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[102]

[98] General Data Protection Regulation (n 57) Art 6 (4) (e), 32 and 34

[99] 'In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage', see General Data Protection Regulation (n 57) Recital (83), Article 6.4. (e), Article 32.1. (a) and Article 34.3. (a)

[100] '"[P]seudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person', see Article 4 (5) GDPR.

[101] 'The application of pseudonymization to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of "pseudonymization" in this Regulation is not intended to preclude any other measures of data protection', see General Data Protection Regulation (n 57) Recitals (26), (28), (29), Article 6.4. (e), Article 25.1., Article 32.1. (a) and Article 89.1

[102] General Data Protection Regulation (n 57) Article 4 (2)

What gives it a special place for ‘the cloud’ is that it triggers the application of the regulation if a cloud provider behaves under the former definition.[103] Meaning that if the cloud provider carries out ‘any operation or set of operations which are performed on personal data', then the regulation applies. At the same time, the GDPR introduces an illustration of examples of processing: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Intrinsically, any sort of clouds, such as IaaS, PaaS or SaaS will conduct a processing performance eventually. Which is why a cloud provider must be aware of the fact that while processing ‘any form of European personal data'[104], this could lead to the enforcement of the GDPR and therefore be subject to responsibility under the European legislation.

2.3.3. The Cloud Service Provider, The Controller And The Processor

Up until now, the cloud service provider (or cloud provider) has been used repeatedly when describing ‘the cloud’. On the other hand, the GDPR does not specifically address neither cloud provider nor ‘the cloud’ as such. The European regulation uses two terms when dealing with the processing of data: the controller and the processor.

The correct assessment of both figures will determine aspects such as the allocation of obligation and liability, the application of the applicable law, and the compliance with other provisions under the GDPR. Both the controller and processor, and the interpretation of their legal status can be used within the processing procedure of cloud services.[105]

Under the scope of the GDPR, ‘“controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such pro-

[103] Staiger (n 79) 100
[104] Staiger (n 79) 101
[105] Ratanachuesakul (n 11) 27

cessing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law', while '"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.[106]

The level of responsibilities and obligations will vary depending on the obligations set out under the GDPR. But the actual functions carried out by the two of them may (at first) appear unclear when describing cloud services. To try to put it in a nutshell, in the processing of cloud services, the most likely situation is the appearance of the cloud service provider, either as a processor or a controller, and the cloud user.[107] By way of illustration, '[i]n a social media context when a user uploads data to a social media site running on a cloud and the provider then alters its advertising based on the personal data received it will be deemed to be a controller'[108] under the GDPR.

For the records, the four main legal scenarios that might be expected to be found in cloud service providers are the processor, the controller, the joint controller, or the neutral intermediary.[109] However, and for the purpose of this paper, it should be mention that these legal statutes are not easily applicable, especially due to the complexity in the business' role of the cloud provider.[110] It may, however, remain as a priority for the cloud provider, to have knowledge of the processing of personal data on its system as well as keep control over it.

At present, it seems necessary to set a uniform definition of when a cloud service provider could acquire the legal status of processor, controller and joint controller, by giving practical examples of common situations, which would provide the necessary guidance[111] in the cloud environment.

[106] General Data Protection Regulation (n 57) Article 4 (7) and 4 (8)
[107] Ratanachuesakul (n 11) 27
[108] Staiger (n 79) 101
[109] Ratanachuesakul (n 11) 27
[110] Ibid 7
[111] Staiger (n 79) 103

2.3.4. Applicability

The applicability of the GDPR is subject to debate, especially when dealing with a matter as complex as cloud services. Generally, the GDPR's material scope 'applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system', but nonetheless 'does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'.[112] Whereas the method of processing is irrelevant, the material scope of the GDPR extends to partly or fully automated processing.

Regarding the territorial scope of the GDPR, it extends to 'the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.[113] When the controller or the processor is not established in the Union, but carries out the processing of personal data of data subjects who are in the Union then, the GDPR applies if 'the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union'.[114] The GDPR adds that '[t]his Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law'.[115] Relevant and important is the fact that the GDPR has expanded the scope of the reg-

[112] General Data Protection Regulation (n 57) Article 2.1 and 2.2
[113] Ibid Article 3.1
[114] Ibid Article 3.2 (a) and (b)
[115] Ibid Article 3.3

ulation to the situation where a non-EU controller or processor 'targets' EU users, and therefore users of 'the cloud'.

In order for a transfer of data to be considered lawful, then there must be provided justification for the purposes of collecting and processing such data, with special consideration to the principles relating to the processing of personal data.[116] Article 6 of the GDPR[117], sets the requirements for lawful processing. In the same line, Article 7[118] of the same regulation, it introduces the conditions of consent, which previously were not included in the DPD. Consent will no longer be classed as freely given where the cloud provider uses default options under which the data subject must object to the processing or when the pre-ticket boxes are used in online forms.[119]

2.4. CASE LAW RELATING TO DATA PROTECTION AND CLOUD COMPUTING

Regarding cloud computing, the Court of Justice of the European Union (hereinafter referred to CJEU) has not issued any specific decision on the field of cloud computing yet. Nevertheless, due to its applicability to 'the cloud' and taking into consideration 'the entire body of case-law available'[120], there are a few cases are worth mentioning. It may be of the interest to add that the decisions of the CJEU are binding throughout the EU.

2.4.1. The Court Of Justice Of The European Union Case Law

Google Spain (C-131/12)

[116] General Data Protection Regulation (n 57) Article 5.1
[117] Ibid Article 6.1
[118] Ibid Article 7
[119] Staiger (n 79) 105
[120] Julien Debussche and Benoit Van Asbroeck, 'Cloud Computing and Privacy Series' (2015) Bird&Bird 7

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González[121] *(Google Spain)* was a case brought before the CJEU in 2014. It has established itself as one of the key data protection cases in the last couple of years in regard to the 'right to be forgotten' and the concept of 'establishment'.

On 5 March 2010, the Spanish national, Mario Costeja González lodged with the AEPD a complaint against *La Vanguardia* Ediciones SL[122], and against Google Spain and Google Inc. In the complaint, Costeja González demanded to the newspaper to erase the information published regarding a 'real state auction connected with attachment proceedings for the recovery of social security debts', which he was involved back in 1998. In the same complaint, he also demanded to Google Inc., or its subsidiary Google Spain, to erase that information from the Google group search engine. This last complaint was based on the fact that when an Internet user entered his name in the search engine, the user obtained links to pages of *La Vanguardia* providing with the information mentioned above. The AEPD denied the newspaper complaint on the ground that the publication was lawful, although upheld the complaint against Google and its subsidiary.

Google Spain and Google Inc, brought separate actions before the National High Court[123] (Audiencia Nacional), who decided to stay the proceedings and to refer the following questions to the CJEU:

'(1) Whether the EU Directive 95/46 as implemented through the national legislation of a Member State can be applied to a foreign Internet search engine company that has a branch or subsidiary with the intent to promote and sell advertising space geared towards the inhabitants of that Member State.

[121] C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* [2014] ECLI:EU:C:2014:317
[122] At the time of the complaint *La Vanguardia* was a daily newspaper with a large circulation, in particular in Catalonia, Spain.
[123] '(...) Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts', see Data Protection Directive 95/46/EC (n 56) Article 28

(2) Whether the Internet search engines' act of locating information published by third parties, and later indexing and making the information available to Internet users can be considered as "processing of personal data" within the meaning of the Directive.
(3) Whether the operator of a search engine must be regarded as a "controller" with respect to the processing of personal data under Article 2(d) of the Directive.
(4) Whether on the basis of legitimate grounds to protect the right to privacy and other fundamental rights envisioned by the Directive, operators of Internet search engines are obligated to remove or erase personal information published by third-party websites, even when the initial dissemination of such information was lawful'.[124]

Firstly, the CJEU taking into account the wording of Article 4 DPD[125] (and the objectives of DPD), held that the processing of personal data carried out by Google Spain fell under the provisions of the Directive, 'when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State'.[126]

Secondly, the Court emphasised the importance of a fair balance between the right to privacy against the right to information access, since search engines are subject to 'affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name'.[127] In the same line, it determined that individuals whose personal data are publicly available through Internet search engines may 'request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results', since the

[124] 'Google Spain SL v. Agencia Española de Protección de Datos' (*Columbia University, Global Freedom of Expression*) in < https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/>
[125] Where 'the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishment complies with the obligation laid down by the national law applicable', see Data Protection Directive 95/46/EC (n 56) Article 4 (1) (a)
[126] C-131/12 (n 121) Paragraph 56-60
[127] Ibid Paragraph 80

rights to privacy and protection of personal data override 'not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name'.[128] The decision of the Court is commonly known as 'the right to be forgotten'.

- **The right to be forgotten applied to cloud computing**

The GDPR has introduced the 'Right to erasure ("right to be forgotten")' in its Article 17.[129] In the light of the complex features of cloud services, it is not easy to understand how some of the grounds for erasure will adapt to 'the cloud'. As previously discussed, the most significant fact lies on defining the subjects involved when engaging cloud services, this means, determine the character of the cloud service providers, as well as its relationship with the data subject. It seems like a number of problems will arise[130] concerning the scope of Article 17, especially in regard to how cloud computing services can comply with the wording of Article 17.

***Lindqvist* (C-101/01)**

Bodil Lindqvist[131] was one of the first cases where the CJEU was asked about the interpretation of the DPD.[132] The Swedish 'Göta' Court of Appeal referred to the CJEU for a preliminary ruling concerning a number of questions, which were raised in criminal proceedings against Mrs Lindqvist before that specific Swedish court.

[128] C-131/12 (n 121) Paragraph 81
[129] General Data Protection Regulation (n 57) Article 17
[130] Francesco Lazzeri, 'The EU's Right to Be Forgotten as Applied to Cloud Computing in the Context of Online Privacy Issues' (2015) Opinio Juris in Comparatione, Vo. I, n.1/2015, Conference Proceedings n. 3
[131] C-101/01 *Bodil Lindqvist* [2003] I – 12992
[132] Data Protection Directive 95/46/EC (n 56)

Mrs Lindqvist was in charged with breach of the Swedish legislation on the protection of personal data for publishing on her Internet site personal data on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church[133].

Regarding the scope of the DPD, the CJEU analysed the processing of personal data in the course of an activity that falls outside the scope of the directive. In this context, it held that trying to distinguish between economic and non-economic activities would end up making 'the field of application of the Directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations'[134]. The CJEU determined that it was the responsibility of both the Swedish government and Courts to take into consideration Mrs Lindqvist right to freedom of expression and then, to contemplate whether her penalty was disproportionate to the offence.

Another point taken into consideration by the CJEU, in this case, was to establish if loading personal data onto an Internet page so that they become accessible to nationals of third countries, constitutes a transfer of data to third countries within the meaning of the DPD. The CJEU held that there was no transfer, by concluding that the state of development of the Internet at the time of DPD was 'drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them'[135]. Nevertheless, the CJEU was very cautious to limit its ruling about transfers, by only considering Mrs Lindqvist's activities.

[133] C-101/01 (n 131) Paragraph 1-2
[134] Ibid Paragraph 41
[135] Ibid Paragraph 68

2.4.2. Case Law In Spain

At the national level, Spain is one of the few Member States that has issued 'cloud-specific' decisions.[136] In concrete, the Spanish Supreme Court has examined a number of claims against the Regulation of Development, Royal Decree 1720/2007, of 21 December, which approved the Regulation implementing the Organic Law 15/1999; in other words, the former Spanish Data Protection Act.[137]

The decision of the Spanish Supreme Court (15 July 2010)

In its decision of 15 July 2010, the Spanish Supreme Court held that whether third-party processors engage in cloud services, additional requirements must be guaranteed: (1) The customer shall be informed of the identification of the outsourcing company (including the country where it develops its services if international data transfer is to take place); (2) The customer can make decisions as a result of the intervention of subcontractors, i.e. it may terminate the agreement or refuse that subcontractors are appointed; and (3) The subcontractors shall enter into a contract that includes guarantees equivalent to those included in the contract with the customer (back-to-back agreements).[138] This way, the Court held that the subcontractor must not only be identified but that its identity must be notified to the client.

AEPD resolution (9 May 2014)

The AEPD has also initiated proceedings in the field of cloud services, such as the Microsoft Corporation cloud solution transfer, issued on 9 May 2014[139], by applying the criteria of the Supreme Court. In the litigation, Microsoft Corporation, parent company of the Microsoft Group placed in the United States, offers cloud computing services called 'Office 365, Mi-

[136] Debussche and other (n 120) 8
[137] Ibid 8
[138] Ibid
[139] AEPD, 'Resolución de declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motive de la prestación de servicios de computación en nube' (TI/00032/2014)

crosoft Dynamics CRM Online and Windows Azure' (hereinafter referred to MOS[140]) through Microsoft Ireland Operations Limited (hereinafter referred to MIOL), placed in Ireland. Thus, the AEPD analysed if the companies involved in the contract fulfilled the lawful requirements for international data transfers, when there is involved a sub processor established in a third country, outside of the European Economic Area (hereinafter referred to EEA).[141]

The standard contractual clauses provided by Microsoft Corporation are those established by the European Commission in its decision 2010/87/EU[142]; with a supplementary agreement for the outsourcing of services in the cloud that focuses on two aspects: conducting audits and subcontracting with the sub-processor. The AEPD concludes that the guarantees provided by Microsoft Corporation may be considered adequate to allow the realization of an international transfer of data in the event that they subscribe to the parties and act as the person in charge of processing. This fact will exempt the undersigned from Microsoft's cloud services from the express authorization of the Director of the AEPD within the framework of international transfers, but not from its notification.[143] The Spanish authority gave the green light for the use of Microsoft's cloud platforms.[144]

- **Personal Data Transfer to a Sub-Processor**

As already mentioned (see 2.2.3. The Cloud Service Provider, the Controller and the Processor), the cloud environment may include a number of different service providers. This being said, these service providers can appear 'often multi-layered' while providing a cloud computing service. From a practical viewpoint, the IaaS provider supplying the necessary hardware to run the software of a SaaS provider for example.

[140] Microsoft Online Services
[141] AEPD (n 139)
[142] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU)
[143] Eduard Puig, 'Nueva resolución sobre transferencias internacionales de datos' (*Faura-Casas*, 26 June 2014) in < http://www.faura-casas.com/es/nueva-resolucion-sobre-transferencias-internacionales-de-datos/>
[144] AEPD (n 139)

In these cases, it is necessary to take into consideration the subsequent processing that takes place. For instance, once the personal data has left the EU. Since the use of sub-processors is a normal practice in the cloud, the GDPR has imposed additional security obligations on processors. The processor must prove that it has retained the right to transfer the data to a sub-processor under its contract with the controller. Additionally, the sub-processor must set the minimum data protection requirements set by the controller in its contract with the processor.[145]

[145] Staiger (n 79) 112-113 and General Data Protection Regulation (n 57) Article 28 '2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller (…)'

CHAPTER 3. THE GENERAL CLOUD COMPUTING POLICY FRAMEWORK

As a result of the increasing interest in cloud computing, many public authorities in the EU have been inspired to adapt themselves and join the movement of 'the cloud'. Cloud computing enables them to achieve 'a higher performance and perform operations' that were not possible before.[146] The way of achieving it, however, has varied in many forms, either through publications or more specifically in guidance. Chapter 3 takes up the subject of cloud computing by providing the most relevant policies and provisions for the matter at the Spanish and European level.

3.1. SPANISH PUBLIC ADMINISTRATION

The effects of the economic crisis and the confluent budget cuts became fundamental for the development of a cloud computing strategy in Spain. During this time of economic crisis, the administration faced the need to find out new formulas, which it would help it to boost its 'international management effectiveness'.[147] As a result, and in line with the Spanish Digital Agenda[148], the public authorities, together with institutions specialised in IT, have released a set of specific documents relating to cloud computing. Among these documents, the most relevant are the 'Spanish National Interoperability Framework' (hereinafter referred to NIF) and the 'Guide for companies: security and privacy of cloud computing'.

[146] Adrian-Mihai Zaharia-Radulescu and Ioan Radu, 'Cloud computing and public administration: approaches in several European countries' [2017] Proceedings of the 11th International Conference on Business Excellence DOI: 10.1515/picbe-2017-0078, pp. 739-749, ISSN 2558-9652

[147] E-Government Observatory, 'Towards a Cloud Computing Strategy in the Public Administration, Sara as a service platform in the cloud' (2013) Ministry of Finance and Public Administration, Government of Spain 1

[148] 'Framework of reference to define a roadmap as regards information and communications technologies (ICTs) and e-Administration; to build Spain's strategy to achieve the goals of the Digital Agenda for Europe; to maximize the impact of public policies on ICT to enhance productivity and competitiveness; and to transform and modernize the Spanish economy and society through efficient and intensive use of ICTs by citizens, businesses and public Administration bodies', see Ministerio de Industria, Energía y Turismo, Gobierno de España, 'Digital Agenda for Spain' (February 2013) in < http://www.agendadigital.gob.es/digital-agenda/Documents/digital-agenda-for-spain.pdf>

NIF was established in the form of a lower level act -a Royal Decree[149]-, published in January 2010 and presenting a global approach to interoperability[150] within the eGovernment legal framework. Mainly, it establishes the principles and guidelines for interoperability in the exchange and the preservation of electronic information by the Public Administration.

NIF has been configured as such in the context of the European Union policies and behaviour in the field. More in detail, interoperability form part of the challenges in 'The Digital Agenda' presented by the Commission; one of the seven pillars of the 'Europe Strategy' for the growth of the EU by 2020. The strategy itself focus on enhancing the interoperability of numerous devices, applications, services, data formats and so on while promoting relevant and suitable rules for intellectual property rights.[151]

A very interesting fact is that many of the services provided to increase the efficiency of the public services, started to be given in the form of cloud computing services, contributing to get closer the regional and local administrations with the central administrative bodies. One of these services is the so-called 'multiPKI validation platform for eID and eSignature' or '@Firma'.[152] But by all accounts, the most relevant service in the matter is the Red 'SARA'.

On 15 January 2013, the High Council for eGovernment, presided by the Ministry of Finance and Public Administration, assigned to SARA the aim to develop the private cloud of the Public Administration in Spain; what it resulted in the first steps towards a cloud compu-

[149] Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope (Friday 29 January 2010 Sect. I. Page 8139)
[150] The ability of disparate and diverse organizations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organizations, through the business processes they support, by means of the exchange of data between their respective ICT systems, see the definition of interoperability according to the Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (no longer in force)
[151] Commission, 'Europea 2020 strategy' in https://ec.europa.eu/digital-single-market/en/europe-2020-strategy
[152] It provides secure services to e-government applications for the creation and validation of electronic signatures, electronic certificates as well as time stamping; it allows the interoperability of electronic signatures and electronic certificates, including electronic signatures created by citizens and business in any eGovernment services, as well as a software product which can be deployed by public bodies with a high demand of signature services, see Miguel A. Amutio, 'The National Interoperability Framework of Spain, a Global Approach to Interoperability Integrated in the eGovernment Legal Framework' (2014) 5

ting strategy and an important interest on 'the cloud' paradigm.[153] As a result, SARA developed into the cloud service: 'Red SARA Cloud'.[154]

SARA helps to interconnect all the Spanish Public Administration -13 ministries, 17 Autonomous Communities, 2 Autonomous Cities, and 3708 local entities-[155]; as well as with the European Union and the other Member States through the 'Trans European Services for Telematics between Administrations'[156] (hereinafter referred to TESTA). Both SARA and TESTA have improved the integration of the Spanish Administration in European cross-border services.

The cooperation goal between all the public administrations in Spain –General State, Regional, Local, Universities, Justice-, has helped to the development of interoperability within the eGovernment scope, but it is worth mentioning with a certain level of complexity. On account of the complexity of such a decentralized territory, the strategy followed to ensue the national interoperability framework has been based on three factors: the support of a sound legal basis; the role of common infrastructure and services; and a strong cooperative effort between public bodies.

Couple with the European network TESTA, the Spanish Public Administration also is member of the Steering Board of the European Cloud Partnership (hereinafter referred to ECP), proposed by the Commission for the development of the European Cloud Strategy.[157] In the same line, it is worth point it out the participation of Spain in the consortium that submitted

[153] E-Government Observatory (n 147)
[154] It provides a set of services and applications for public administrations intended to facilitate the sharing of services and infrastructures to reduce operating costs and investment needs, see Miguel A. Amutio, 'The National Interoperability Framework of Spain, a Global Approach to Interoperability Integrated in the eGovernment Legal Framework' (2014) 4-5
[155] Miguel A. Amutio, 'The National Interoperability Framework of Spain, a Global Approach to Interoperability Integrated in the eGovernment Legal Framework' (2014) 4
[156] It provides a European backbone network for data exchange between a wide variety of public administrations, by using Internet Protocols (IP) to provide universal reach, but operated by the Commission separately from the Internet. It provides guaranteed performance and a high level of security and has connections with the EU Institutions and national networks, see Definition of TESTA by the Commission in https://ec.europa.eu/isa2/solutions/testa_en
[157] Commission (n 6)

the proposal to the EU Framework Programme 7 (hereinafter referred to FP7) for the provisioning of cloud computing services based on pre-commercial procurement models[158]; this, in order to help the stimulation of the European cloud computing network from the public sector.

The different documents have shown thus now that the Ministry of Finance and Public Administration is in charge of the migration of public services into 'the cloud'[159]. Under this Ministry, it was also created the Commission for the Reform of Public Administration (hereinafter referred to CORA). The role of CORA has been to promote the necessary reforms within the public administration that would lead to higher efficiency in delivering public services and support economic growth.[160] In light of all these facts, the Spanish public administration has proved the necessity to develop and use cloud computing as a key mechanism to promote business competitiveness, with the public sector as the driven force and the establishment of guidelines for advising and cooperating with the private sector.[161]

The National Institute of Communications Technology of Spain[162] (hereinafter referred to INTECO) has also developed the so-called 'Guide for companies: security and privacy of cloud computing'.[163] The guideline sets up the different levels of clouds, which services are deployed and which regulatory framework is of reference, among many other aspects. Likewise, it has been designed specially to help companies, particularly small and medium-sized enterprises (hereinafter referred to SMEs), with their security and implementation policies.[164] The Institute also provided with the lifecycle of data when processing in the cloud[165]

[158] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2007) 799 final) Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe {SEC(2007) 1668} [2007]
[159] Zaharia-Radulescu and other (n 146)
[160] Ibid
[161] E-Government Observatory (n 147)
[162] It is the National Institute of Communication Technology based in León, Spain. It is affiliated to the Ministry of Industry, Tourism and Trade through the State Department of Telecommunications and Information, see Joyanes (n 3) 94
[163] INTECO, 'Guía para empresas: seguridad y privacidad del cloud computting' (2011) Ministry of Finance and Public Administration, Government of Spain
[164] Joyanes (n 3) 94

and proposes a mechanism to decrease any privacy risks. Before concluding, it should be noted that the guide provides with the key elements for companies to achieve the best results while using cloud-computing services.[166]

3.1.1. Guidance Provided By The AEPD

In addition to the former policy guidelines, at a national level, the different DPAs have also released guidelines on cloud computing. In the case of Spain, the most relevant documents published by the AEPD are "Guide for clients using Cloud computer services" and "Guide for Cloud service providers. These guidelines focus on key matters. Both guides are available in Spanish at the DPA's website.

The Guidelines highlight aspects already mentioned in the prior Chapter: (1) Content Service Provider (CSPs) shall be considered data processors; (2) Users shall be informed of the identification of services and the outsourcing company (including the country in which it develops its services if international data transfers are to take place); (3) Users can make decisions as a result of the intervention of subcontractors, for instance, they may terminate the contract or refuse that the subcontractors are appointed; (4) CSPs and subcontractors shall enter into a contract that includes guarantees equivalent to those included in the contract with the customer.[167]

---

[165] Data is prepared for the cloud by changing its format or creating a file with all the information required. The data 'travels' to the cloud over an Internet connection, using email, a specific application or transferring a backup copy to the cloud. Data is processed in the cloud, from storage to complex mathematical operations. Backup copies can be stored on the cloud for future access. The resulting data 'travels' back to the user. When processing is complete, the data should be returned to the user with the added value of the information generated in the cloud. Data may represent a risk to privacy when leaving the organization: A person with malicious intentions could intercept data during transfer. However, the data is stored and processed in an IT infrastructure that is outside the user's control, see Joyanes (n 3) 94

[166] Debussche and other (n 120)

[167] Debussche and other (n 120) 7, and see (epigraph 2.3.2. Case Law in Spain, *AEPD resolution (9 May 2014))*

3.2. EUROPEAN UNION

In the European Union, the interest to start working in the digital phenomenon goes back to the last century, specifically to the 80s.[168] Ever since the Commission has launched a few public policies focusing on different aspects such as the promotion of digital interoperability (see epigraph 3.1.).

The Digital Agenda[169] introduced the first steps on the basis of cloud computing, in particular, in the Communication of the Commission 'Unleashing the Potential of Cloud Computing in Europe'.[170] In Commission's own words, 'Where the World Wide Web makes information available everywhere and to anyone, cloud computing makes computing power available everywhere and to anyone'.[171] In the Communication, it is acknowledged that cloud computing can cut ICT costs if combine with new 'digital business' practices. It also sets its tremendous potential, meaning EUR 45 billion of direct spend on Cloud Computing in the EU in 2020 as well as an overall cumulative impact on GDP of EUR 957 billion, and 3.8 million jobs, by 2020.[172]

In closer detail, the document establishes a sort of strategy for encoring the use of cloud computing across all economic sectors, which it results in the study of the overall policy, regulatory and technology scenery. Through its strategy, the Commission determines the most important and urgent three cloud actions: safe and fair contract terms and conditions;

[168] Silvia Serrano Calle, Jorge Pérez Martínez and Zoraida Frías Barrosa, 'Spanish Public Policies towards the Promotion of Cloud Computing and Digital Services for SMEs' [2016] 27th European Regional Conference of the International Telecommunications Society (ITS), Cambridge, United Kingdom 3

[169] 'The Digital Agenda is established as one of the seven pillars of the Europe 2020 Strategy, which sets objectives for the growth of the European Union (EU) by 2020. It proposes to exploit the potential of Information and Communication Technologies (hereinafter referred to ICTs) in order to foster innovation, economic growth and progress. The Digital Agenda's main objective is to develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe', see Commission (n 151)

[170] Commission (n 6) 2

[171] Ibid

[172] Ibid

cutting through the jungle of standards; and establishing a European cloud partnership[173] to drive innovation and growth from the public sector.[174]

Key action relating to 'safe and fair contract terms and conditions' arises from the need to safeguard different concerns over data access and portability, change control and ownership of the data. More in detail, 'how liability for service failures such as downtime or loss of data will be compensated, user rights in relation to system upgrades decided unilaterally by the provider, ownership of data created in cloud applications or how disputes will be resolved'.[175]

Second key action regards to cutting a 'jungle of standards'. This measure is taking into consideration since there were uncertainties regarding 'which standards provide adequate levels of interoperability of data formats to permit portability; the extent to which safeguards are in place for the protection of personal data; or the problem of the data breaches and the protection against cyber attacks'.[176]

The last key 'cloud-specific' action, in regard to the establishment of a European Cloud Partnership, stems from the necessity of providing clearness 'due to differing national legal frameworks and uncertainties over applicable law, digital content and data location ranked highest amongst the concerns of potential cloud computing adopters and providers. This is in particular related to the complexities of managing services and usage patterns that span multiple jurisdictions and in relation to trust and security in fields such as data protection, contracts and consumer protection or criminal law'.[177]

The Commission also launched a comparative legal study on cloud contracts as a follow-up to the Communication. The study carried by DLA Piper provides with legislation, case law and administrative guidelines applicable to cloud computing contracts. The study concludes

[173] Debussche and other (n 120)
[174] Commission (n 6) 10
[175] Commission (n 6) 5
[176] Ibid
[177] Ibid

that no specific 'cloud laws' exist all Member States. Nevertheless, many sector-specific regulatory initiatives have been published. These may help to increase the interest in national cloud regulations.[178]

On 10 December 2013, the Parliament adopted the resolution on unleashing the potential of cloud computing in Europe.[179] The document takes into consideration the Commission Communication of 27 September 2012, among many others documents, and examines the strategies proposed, by adding that, 'in order to achieve the ambitious goals set out by the strategy, a legislative instrument would have been more adequate for some aspects'.[180] Generally, the resolution examines the Digital Agenda and the diverse tools in the field of ICT, by setting the main challenges and issues: the cloud as an instrument for growth and employment; the EU market and the cloud; public procurement, and procurement of innovative solutions; standards; consumers and the cloud; intellectual property, civil laws, etc.; and data protection, fundamental rights and law enforcement.[181]

In July 2014, the Commission Staff published the Report on the Implementation of the Communication 'Unleashing the Potential of Cloud Computing in Europe' accompanying the Communication '[t]owards a thriving data-driven economy'.[182] The legal basis of the Report is to show the progress on the set of policy actions set in the Communication, to report on the results of the state of play regarding on-going actions and the foundation for further follow-up actions in the field of cloud computing.[183]

---

[178] Commission, 'Comparative study on cloud computing contracts' in < https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/study-cloud-computing-contracts_en>
[179] European Parliament Resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe (2013/2063(INI))
[180] Ibid
[181] Debussche and other (n 120)
[182] Commission Staff Working Document SWD(2014) 214 final Report on the Implementation of the Communication 'Unleashing the Potential of Cloud Computing in Europe', *Accompanying the document* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Towards a thriving data-driven economy' {COM(2014) 442 final} [2014]
[183] Ibid 2

As regards the implementation of the three key actions for the European Cloud strategy, it was created the 'Cloud Select Industry Group'[184] (hereinafter referred to C-SIG), which supported the implementation of the key actions. Up to this date (January 2019), the last plenary published of the C-SIG was in 2017. The plenary addressed the most recent developments in cloud computing, with special emphasis on the topic of 'free flow of data'. With the intention to address the different types of data and its flow across borders; the Commission introduced the topic in the Policy Communication 'Building a European Data Economy'.[185]

After the publication of the Communication 'European Cloud Initiative – Building a competitive data and knowledge economy in Europe[186], the Commission intends to launch another study at assessing problems encounter in relation to cloud computing contracts. In a nutshell, all the cloud computing policies have been introduced within the Digital Single Market Strategy for Europe, playing a special key role the European Cloud Initiative, and the European Free Flow of Data Initiative.

[184] C-SIG is open to all organisations, groups and individuals having a professional interest in cloud computing matters and are active in the European cloud market. It was created by the Directorate-General for Communications Networks, Content and Technology, Software and Services, Cloud Unit, with representatives from major European and multinational companies and organizations with significant involvement in cloud computing, for the purpose of providing independent validation and advice on proposals, see Commission, 'Cloud Select Industry Groups' in < https://ec.europa.eu/digital-single-market/en/cloud-computing-strategy-working-groups>
[185] Commission, 'Cloud Select Industry Group – First plenary meeting in 2017' in < https://ec.europa.eu/digital-single-market/en/news/cloud-select-industry-group-first-plenary-meeting-2017>
[186] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2016) 178 final) European Cloud Initiative - Building a competitive data and knowledge economy in Europe {SWD(2016) 106} {SWD(2016) 107} [2016]

CONCLUSSIONS

- Chapter 1 takes into consideration the nature, most standard definition and main characters and stakeholders of cloud computing, while determining the different service models –SaaS, PaaS and IaaS- and ascertain the division made between the cloud computing deployment models –private, public, community and hybrid-. Despite its complexity nature, the versatile characters of cloud computing makes it a very attractive business. This statement ended with a brief presentation of the benefits of 'the cloud'. Business, individuals and governments can benefit by renting cloud services and storing data without spending huge amounts of money on equipment and software.

- Nevertheless, balancing cloud benefits and security duties is therefore a critical success factor when engaging cloud services. Besides, new technologies can be ruled to varied forms of legally safeguards and boundaries. As with the transition of data from the analogue to the digital domain, data protection raises big concerns due to the massive concentrations of personal data in an environment of people and devices interconnected by the Internet. Chapter 2 took up the study of data protection, by analysing the current regulation across the EU through the GDPR, with special emphasis in the particularities of the Spanish data protection regulation. The GDPR has been the most relevant milestone on data protection in recent times. It could be argued, whether the exigent data protection laws in the EU may be depriving the use of 'the cloud'. On the other hand, the lacking of an exigent data protection regulation would lead to higher risks. Nevertheless, it should remains that cloud computing is beyond the reach of current data protection laws and the GDPR is holding a period of change 'in IT law and regulation as business transforms through the adoption at scale of new technology (…) Nowhere is this more clearly shown that in the legal aspects of the rapidly developing area of cloud security'.[187] Besides, key legal issues have been discussed in literature, but mostly from the perspective of the cloud service business and not from the viewpoint of the data subject. The main is reason is the great demand that arises the cloud service

[187] Richard Kemp, 'Legal Aspects of Cloud Computing: Cloud Security' (2018), Insight and Thought Leadership Service, White Papers.

provider as a fast-growing business. New legal approaches will have to deal with the current gap between the legitimate interest of individuals and the business model of 'the cloud'.

- Notwithstanding, the scope and applicability of the GDPR for cloud computing services seems unclear. This is mainly to ambiguous definitions and lack of a more detailed regulation in the matter. It seems appropriate an agreement upon standards in regard to different concerns, such as the identifiability of personal data and the definition of cloud computing providers within 'the cloud' environment. This would bring legal certainty. This being said, it seems appropriate to take advantage of the lack of domestic rules at the national level, to set cloud computing standards across the EU. Same as it happened with the GDPR, a European cloud regulation would be possible. Moreover, the truth is that any technological development poses new challenges, especially to its own regulation, without forgetting the complexity of the matter it has been discussed.

- Chapter 3 presented that both the EU institutions and the public Administration are aware of the tremendous benefits of engaging in 'the cloud' paradigm. Beyond pure costs saving, the implementation of cloud computing is helping to improve service performance in line with the needs of more a more technological demanded businesses and population, not to mention the objectives set for the European digital single market. As way of illustration, to improve 'service performance such as improved security, more user-friendly services, the ability to roll out new services cheaply, fast and flexible, the relative ease of using cloud computing for creating social engagement platforms or for specific campaigns and the scope to monitor outcomes better. But looking forward ten years cloud could help realise the vision of 'Every European Digital', able to enjoy full electronic public services rather than a paper bureaucracy. Cloud computing could help to drive public costs down and push public benefits up and give a broader base for economic activity involving the whole population'.[188]

[188] Commission (n 6) 5

BIBLIOGRAPHY

Legislation and Related Texts

-Spanish Constitution of 1978 (as amended on August 28, 1992)

-Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope (Friday 29 January 2010 Sect. I. Page 8139)

-Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE-A-2018-16673)

General Guidelines

-ENISA, 'Cloud Computing. Benefits, risks and recommendations for information security' (2009)

-INTECO, 'Guía para empresas: seguridad y privacidad del cloud computting' (2011) Ministry of Finance and Public Administration, Government of Spain

-E-Government Observatory, 'Towards a Cloud Computing Strategy in the Public Administration, Sara as a service platform in the cloud' (2013) Ministry of Finance and Public Administration, Government of Spain

-OECD, 'The OECD Privacy Framework' (2013)

-Agencia Española de Protección de Datos, 'Criterio de la Agencia Española de Protección de Datos sobre cuestiones electorales en el proyecto de nueva LOPD', (2018)

European Legislation

-Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)

-Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Decisions

-Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU)

-Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (no longer in force)

Communications

-Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM(2010) 609 final A comprehensive approach on personal data protection in the European Union [2010]

-Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM (2012) 529 final Unleashing the Potential of Cloud Computing in Europe [2012]

-Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2007) 799 final) Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe {SEC(2007) 1668} [2007]

-Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2016) 178 final) European Cloud Initiative - Building a competitive data and knowledge economy in Europe {SWD(2016) 106} {SWD(2016) 107} [2016]

Opinions

-Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (01248/07/EN WP 136)

-Article 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' (WP 196, 1 July 2012)

Resolutions

-European Parliament Resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe (2013/2063(INI))

-AEPD, 'Resolución de declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motive de la prestación de servicios de computación en nube' (TI/00032/2014)

Others

-Commission Staff Working Document SWD(2014) 214 final Report on the Implementation of the Communication 'Unleashing the Potential of Cloud Computing in Europe', *Accompa-*

nying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Towards a thriving data-driven economy' {COM(2014) 442 final} [2014]

Case Law

European Court of Justice

-C-101/01 *Bodil Lindqvist* [2003] I – 12992

-C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* [2014] ECLI:EU:C:2014:317

Bibliography

Books

-Cheung, Anne S.Y. and Weber, Rolf H., *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016)

-Cheung, Anne S. Y., 'Re-personalizing personal data in the cloud' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016)

-Chang, H. 'Data Protection regulation and cloud computing' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016)

-Staiger, Dominic N., 'Cross-border data flow in the cloud between the EU and the US' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016)

-Xiaoxi Fan, Joe Kong and Chow, K.P., 'Introduction to cloud computing and security issues' in Anne S.Y. Cheung and Rolf H. Weber, *Privacy and Legal Issues in Cloud Computing* (Elgar Law, Technology and Society, Edward Elgar Publishing Limited 2016)

Articles and Papers Published

-Altieri, L. and Cifaldi, G., 'Big data, privacy and information security in the European Union' (2018), Sociology and Social Work Review, 57

-Bermejo Bosch, R. and López-Lapuente, L., 'The Privacy, Data Protection and Cybersecurity Law Review' [2017] The Law Reviews, The Privacy, Data Protection and Cybersecurity Law Review - Edition 4

-Greenleaf, G. 'Global Data Privacy Laws 2013: 99 Countries and Counting' (2013), 123 Privacy Laws and Business International Report 10

-Joyanes Aguilar, L., 'Cloud Computing Notes for a Spanish Cloud Computing Strategy' (2012) Journal of the Higher School of National Defence Studies

-Kemp, R., 'Legal Aspects of Cloud Computing: Cloud Security' (2018), Insight and Thought Leadership Service, White Papers

-Kuan Hon, W., 'Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens' (2017), Edward Elgar Publishing

-Kuan Hon, W., Kosta, E., Millard, C. and Stefanatou, D., 'Cloud Accountability: The likely impact of the Proposed EU Data Protection Regulation' (2014) Queen Mary School of Law Legal Studies Research Paper 172/2014, 10-13

-Kuan Hon, W., Millard, C. and Walden, I., 'The problem of "Personal Data" in Cloud Computing' (2011) 1 IDPL 211-215

-Lazzeri, F., 'The EU's Right to Be Forgotten as Applied to Cloud Computing in the Context of Online Privacy Issues' (2015) Opinio Juris in Comparatione, Vo. I, n.1/2015, Conference Proceedings n. 3

-Mell, P. and Grance, T., 'The NIST Definition of Cloud Computing' (*National Institute of Standards and Technology Information Technology Laboratory,* 2011) Special Publication 800-145

-Pauner, C. and Viguri, J., 'The Adaptation Of The GDPR In Spain: The New Data Protection Act (LOPD)' (2018), E-conférence, National Adaptations of the GDPR

-Serrano Calle, S., Pérez Martínez, J. and Frías Barrosa, Z. 'Spanish Public Policies towards the Promotion of Cloud Computing and Digital Services for SMEs' [2016] 27th European Regional Conference of the International Telecommunications Society (ITS), Cambridge, United Kingdom 3

-Zaharia-Radulescu, A. and Radu, I., 'Cloud computing and public administration: approaches in several European countries' [2017] Proceedings of the 11th International Conference on Business Excellence DOI: 10.1515/picbe-2017-0078, pp. 739-749, ISSN 2558-9652

Theses

-Ratanachuesakul, C., 'The Legal Status of a Controller and a Processor of a Cloud Service Provider Under the GDPR in the Context of the Complete Protection to the Data Subject' (Thesis, Tilburg Institute for Law, Technology and Society (TILT) LL.M. Law and Technology, 2017-2018)

-Schellekens, B.J.A., 'The European Data Protection Reform in the Light of Cloud Computing' (Master Thesis, University of Tilburg 2013)

Online Articles and Blogs

-Amutio, M.A., 'The National Interoperability Framework of Spain, a Global Approach to Interoperability Integrated in the eGovernment Legal Framework' (2014)

-Bru, P. and Fernández Longoria, P., 'Spain finalises new data protection and digital rights law' *Out-Law.com* (27 November 2018)

-Debussche, J. and Van Asbroeck, B., 'Cloud Computing and Privacy Series' (2015) Bird&Bird

-Puig, E. 'Nueva resolución sobre transferencias internacionales de datos' (*Faura-Casas*, 26 June 2014)

-Forni, A.A., and Van der Meulen, R., 'Gartner Says By 2010, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today' *Gartner* (Stamford, Conn., June 22 2016)

-'Google Spain SL v. Agencia Española de Protección de Datos' (*Columbia University, Global Freedom of Expression*)

-Kelly, M., 'These 5 countries were ranked best for privacy (infographic)' *Venture Beat* (13 October, 2013)

-Natsui, T., 'Cloud Computing Service and Legal Issues' Meiji University, Tokyo, Japan

-Peguera, M., 'New Spanish Law Raises Concerns Over Use Of Sensitive Data By Political Parties', (Standford Law School, The Center for Internet and Society, 24 November 2018)

-'Spain approves contested data protection law', *Mail & Guardian* (22 November 2018)

-Sampedro, G. and Vidal, E., 'A new Data Protection Act for Spain' *Bird & Bird* (December 2018)

Websites

https://ec.europa.eu/digital-single-market/en/news/cloud-select-industry-group-first-plenary-meeting-2017

https://ec.europa.eu/digital-single-market/en/cloud-computing-strategy-working-groups

https://ec.europa.eu/info/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/study-cloud-computing-contracts_en

https://ec.europa.eu/isa2/solutions/testa_en

https://ec.europa.eu/digital-single-market/en/europe-2020-strategy

http://www.agendadigital.gob.es/digital-agenda/Documents/digital-agenda-for-spain.pdf

https://en.wikipedia.org/wiki/Data_Re-Identification

https://www.gartner.com/en/about

https://www.nist.gov/about-nist

https://en.wikipedia.org/wiki/Information_technology#cite_note-2

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority_en

https://www.aepd.es/reglamento/cumplimiento/principio-responsabilidad-proactiva.html

https://www.aepd.es/prensa/2018-06-11.html

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en

ABSTRACT

As the technological revolution evolves rapidly, cloud computing is becoming a component of everyone's daily life. This is explained by an unprecedented proliferation of data on 'the cloud'. Processing data and utilizing storage platforms is easily accessible both at low cost and high efficiency. Yet, whilst cloud computing provide with a unique convenience, it has also led to unseen challenges especially on the field of data protection. This paper analyses the most relevant legal issues when engaging cloud services, by taking the General Data Protection Regulation and the different policy guidelines provided by the EU institutions into consideration, as well as the Spanish public administration in recent years.

Keywords

Cloud Computing, Internet, Personal Data, Data Protection, European Union, Spain, General Data Protection Regulation

KURZFASSUNG

Im Rahmen der gegenwärtigen rasanten technologischen Revolution wird Cloud Computing zu einem Bestandteil des alltäglichen Lebens, aufgrund dessen eine weitreichende Verbreitung von Daten in „der Cloud“ stattfindet. Die Verarbeitung von Daten und die Verwendung von Speicherplattformen ist mit hoher Effizienz und bei geringen Kosten möglich. Cloud Computing-Services bieten einen einzigartigen Komfort, führen jedoch insbesondere im Bereich des Datenschutzes zu ungeahnten Herausforderungen. Dieses Dokument kann nicht die gesamten Implikationen dieses Konfliktes darstellen. Allerdings werden die relevantesten rechtlichen Fragen bei der Nutzung von Cloud-Diensten unter Berücksichtigung der allgemeinen Datenschutzverordnung und der verschiedenen politischen Richtlinien, die von den EU-Institutionen und der spanischen öffentlichen Verwaltung in den letzten Jahren bereitgestellt wurden, analysiert.

Schlüsselwörter

Cloud Computing, Internet, Persönliche Daten, Datenschutz, Europäischen Union, Spanien, Datenschutz-Grundverordnung