The European Strategy for Cloud Computing: Harmonization of Technical and Legal Rules

Caterina Flick, Vincenzo Ambriola

Abstract. *Cloud computing is an emerging technology that aims to reduce the cost of software services and resources. The basic idea is to move computational power and data storage from the client to the server, thus improving quality of service, enhancing safety levels, and allowing a better allocation of resources. The widespread diffusion of Internet and the rapid acceleration of the use of smart mobile devices have shown that cloud computing solutions are not only possible but somehow inevitable. In this new scenario the European Union has developed a strategy for adopting cloud computing and exploiting its potential. In this paper we present the theme that characterizes this strategy: harmonization of technical and legal rules. The focus on legal rules is of paramount importance for the profound impact that cloud computing can have on our society. We will discuss the following aspects related to data stored in the cloud: access and integrity, property, storage and transfer. Particular attention will be devoted to the adoption of cloud computing in the public administration.*

Keywords: Cloud computing European Union strategy, standards and rules, public administration.

1. Introduction

Cloud computing is the centralization of infrastructures, platforms, and programs and their redistribution to end-users through Internet. The centralization of data repositories and processes for their provision allows such a scale economy that even large companies alone cannot achieve. For this reason, the adoption of cloud computing can lead to substantial savings in IT budgets, and pave the way for the solution of technical and economic problems related to existing IT systems.

Although one of the fastest growing IT industries in the world, cloud computing is a technology almost unknown to the majority of European citizens: less than a quarter of them, in fact, uses cloud services. In addition, its use is much more common for personal needs than for business reasons.For many companies, on the other hand, the transition to cloud computing is perceived as an important opportunity to reduce the costs of IT infrastructures. The anticipated savings would mainly derive from the ability to purchase computing resources and

services from third parties, without having to purchase and maintain expensive and complex IT systems. According to a study commissioned by Microsoft [Forum PA, 2012], the revenues from cloud computing business may be high (832 billion Euro over the next three years) and new jobs could have a significant impact on employment (152,000 in Italy, with an increase of 125%).

The sustainability of cloud computing depends on simplification and harmonization, both in technical and legal terms: tools easily accessible, flexible and affordable contractual instruments, full control of data (for reasons of security and privacy), effective exercise of rights.

2. The European strategy for cloud computing

The strategy adopted by the European Commission on September 27, 2012 has the aim to accelerate and increase the use of cloud computing. This strategy is the result of a wide-ranging analysis of the political aspects, regulations, and technology in the member countries, followed by an extensive consultation aimed at identifying all the potential offered by cloud computing. The strategy is divided in three main objectives.

The first objective aims to simplify and eliminate the "jungle" of technical standards, with the aim of allowing users to enjoy interoperability, data portability and reversibility. The Commission will work with the support of ENISA and other organizations to provide assistance to the development of voluntary certification schemes, providing a list by 2014 (the list of high-level criteria and the first list of certification schemes has been released by CERT-SIG on November 2013). The second objective is to develop security models and conditions of use that are accessible (fair), uniform, and easy to apply and interpret. The third objective is to identify a European partnership to drive innovation and growth of the public sector. This will be achieved by bringing together experts from industry and the public sectors that will work on the definition of common requirements for the purchase of cloud computing services, in an open and fully transparent way. The public sector, in particular, has a key role in the development of the cloud computing market. In the presence of a fragmented market, in fact, this requirement will have a minimal impact on the public sector, since the integration of services would be low and the citizens would not get the best results at the lowest cost (best quality/price ratio).

Neelie Kroes, European Commissioner for the Digital Agenda, has repeatedly stressed the importance of cloud computing for European economic growth and announced a European Cloud Partnership (with an initial investment of 10 million Euro) to start building a solid foundation for the joint procurement of cloud by the public authorities. According to data provided by the Commission, this opportunity can generate 800,000 jobs and economic benefits for more than 200 million Euro. The indirect benefits induced by the adoption of cloud computing are endless, especially for public services, which can be made more efficient and affordable, with great benefits for the European population.

The existence of a digital market, globally integrated and cohesive, will give users the freedom to choose between different services. In addition, the

European service providers can take advantage of these opportunities to grow even beyond the European borders. In the coming months, the European Commission should indicate a harmonized regulatory framework, which aims to promote the use of cloud computing in enterprises and public administrations. The difficulty in finding such a framework depends on the multiplicity of visions and different laws between member states, in particular on important issues related to security, privacy, and transparency.

Among others, the European Commission should focus on legal issues involving privacy, data retention, applicable law, liability, and consumer protection. Other important issues that need be taken into account are those related to interoperability, standardization, data portability. As regards the public sector, in addition, there is a need to define precise rules for choosing suppliers and entrusting the management of services.

3. Simplification of technical standards

The simplification of technical standards is intended to provide users with interoperability, data portability, and reversibility. A change of this kind, however, must be accompanied by proper regulation of the rules of intellectual property and licensing. The existence of a multiplicity of technical standards, combined with the use of rigid rules on intellectual property, may in fact lead to restrictive effects on competition, either by preventing the lowering of prices, limiting or controlling production, market, innovation, and technological development.

First, if cloud computing producers are involved in a conflict in the context of anti-competitive standards there is a risk that this will lead to less price competition, facilitating agreements between parties who are outside the market.

Secondly, the identification of technical standards (often very detailed) for a product or service may limit development and technological innovation. At the moment in which a standard is being developed, alternative technologies can compete for inclusion in the standard. Once a technology has been chosen and the standard has been identified, different technologies and manufacturers may face unfair restrictions and could potentially be excluded from the market.

Thirdly, standardization can lead to results which are contrary to competition, where they place limits on some players with respect to the capacity of effective access to the results of the process that led to the identification of the standard.

In recent years, the European Commission has revised the rules for horizontal cooperation agreements in the light of the European competition law, including the guidelines on the implementation of Article 101 of the Treaty on the Functioning of the European Union. The Commission has also addressed the issue of licenses for ICT and finally, in November 2012, the implementation of Open Source standards. A working group for the detection of certification schemes started to work in February 2013.

Simplification requires special attention. For portability services, simplification is the ability to seamlessly migrate applications, virtual machines, and data from a cloud computing environment to another. To make this possible it is necessary that the two environments (departure and arrival) be highly interoperable,

because the same application environment can be replicated by different suppliers. Interoperability, however, is also the opportunity to share the same management tools, virtual machines, and other resources, including a plurality of service providers and cloud computing platforms. Portability should make data and programs "understandable" even by a receiving system, made available by another cloud service provider, regardless of the specific characteristics of the hardware and software platforms used.

In late 2013 the CERT-SIG (ENISA) elaborated a list of guiding principles for certification schemes for cloud providers. These principles are connected with – *inter alia* – technological neutrality, global standards and affordability. The definitive list of schemes should be released on 2014.

4. Consistent, secure, and simple legal rules

During the European Conference on Cloud Computing, which was held on March 7, 2013 in Brussels, was raised the question of defining a legal framework to create a market for cloud computing services. The obstacles to a uniform regulation of the terms and conditions of the contract for the provision of these services derive, in fact, from the differences in this area between national laws. It is therefore necessary to develop a model of contractual terms that cover matters not governed by European legislation in the field of contracts, such as data retention after contract expiry, access and integrity of data, location and data transfer, data ownership, direct and indirect responsibility in the management of cloud computing service from suppliers and sub-contractors.

5. Data access and data integrity

The availability of data, and accessibility at any time, requires the assurance of quality standard of the connectivity provided by Internet. Without this quality requirement, cloud computing services may be degraded by traffic peaks, or even made unavailable by abnormal events (failures, for example). This aspect depends only in part by the cloud computing providers, as it involves the highest level of political bodies and government, responsible for the organization, the diffusion, and the management of Internet.

The accessibility of data requires to preserve its integrity, with an explicit focus on deletion or damage. It is also necessary to take appropriate security measures to protect data confidentiality, especially with regard to visibility or use by unauthorized persons. In a nutshell, from the legal point of view, it is necessary to refer to the rules on privacy, or to the Legislative Decree no. 196/03 and a number of European directives, in particular Directive 95/46/EC and the recently adopted Regulation 611/2013, in force since August 25, 2013, on mandatory reporting of violations of privacy.

Data confidentiality largely depends on the security mechanisms used by the supplier. This technical aspect, however, does not relieve public and private entities that use a cloud computing service to manage their information assets or, even more, data and information on behalf of third parties, from their responsibilities. It is implicitly stated that they must take appropriate measures to

ensure the security of data and information handled by these services. In the case of treatment of personal data, the entity in charge of a cloud infrastructure continues to be responsible for the adoption of security measures, as it holds the position of "owner" of the treatment. At the same time, all the obligations related to information security associated with the commission of crimes during the execution of a service, which lead to a direct responsibility in charge of providing the service, are part of the measures envisaged by the 2001 European Convention on Cybercrime.

The provider of a cloud computing service must guarantee data security in a transparent manner, taking care of correct data transmission and storage, including the adoption of safe and regular back-ups. Technical and organizational infrastructure aspects of a cloud computing framework, including its overall design, the development process of provided services, the configuration of the transmission systems, the adoption of specific contracts with users and sub-contractors, the systems that control access requests, have an essential role in the objective of ensuring data security.

The need to protect data from intruders and unauthorized uses imposes a limit to the amount of information about users, traffic, property. This could be in conflict with the need both to make data rapidly and continuously available to users, and to react quickly in an emergency. This requirement is also in contrast of the need for confidentiality (or rather the interest in not being controlled) of those who are authorized to access. In case of system faults, in fact, the accuracy and timeliness of diagnosis and remedy are closely related to the completeness of the available information. In addition, as many faults and anomalies involve multiple vendors, the resolution of a problem may require cooperation between several parties, potentially residing in different states.

In summary, a system that safeguards data security and confidentiality has two objectives: on the one hand it must be able to detect an attack as quickly and accurately as possible and should react just as quickly, to maintain the levels of quality of services provided, on the other it must ensure the confidentiality of the users involved and whose actions are monitored. A reduction of user data can increase the level of confidence, ensuring infrastructure recovery operations. Similarly, increasing the available data, a high level of protection can be easier to accomplish. A solution that that solves this dilemma is based on the use of advanced encryption techniques.

6. Data property

Moving data to a cloud service provider requires to clearly define the notion of data. This is an issue that directly involves both intellectual rights and industrial property, with some complications that arise from the difficulty of identifying the place where data are stored.

With particular reference to creative works, still ruled by the Italian law on copyright 633/1941 which reflects only in part the characteristics of Internet, it is imperative to point out that dematerialization of media storage and preservation of these works can raise new and relevant questions. When creative works are

transmitted to a cloud computing provider (on a physical media that he owns) the way these works are used immediately changes, since they could be made available to multiple users through an on-demand access from multiple locations, with the permission of the author, but also to his knowledge.

On the other hand, the concentration of data in the hands of individual market participants, who are not involved in providing creative works on Internet but that simply allow their diffusion, requires, in order to protect the author rights, to break down the evident state of irresponsibility of the service provider. Without taking into account this aspect, service providers would not respond for content uploaded by users. For the author of a creative work would be difficult and expensive to identify those who, in theory, have violated his rights (an activity made even more complex by coordination with the legislation on privacy). The conflict between different interests has been brought in an Italian court, with the so called *Peppermint versus others*. In this case, the argument was the protection of copyright, owned by Peppermint, against the protection of the privacy of Internet users.

In the absence of regulatory changes, including the obligation on a provider of telecommunications services, there is only a duty to inform the supervising judicial or administrative authority, in relation to reliable information received in respect of the infringement of copyright accomplished through telecommunications network. There is no obligation to terminate the service provided by providers, even when there is evidence of unlawful acts whose effect is to make available some content that infringes copyright.

Another issue of great importance about data ownership reflects the requirements related to personal data processing, both during the contractual relationship and at its termination, in relation to the compulsory destruction of data held by the supplier. In general, it is sufficient to say that the principles established for the protection of personal data must be adapted for the use of cloud computing services, i.e. taking into account the problems associated with the peculiarities of such systems. More specifically, it is necessary to address the issue of the obligations in charge of the supplier, treating this actor as someone other than the owner of data, and appointed by him responsible, with respect to the discretionary powers resulting from the treatment of the data. The issue needs to be addressed with particular attention when the data entrusted by the user of the infrastructure provider are related to third parties: this is the case, for example, of public administrations, which collect citizens' data, as well as those of its employees.

7. Location and data transfer

The theme of the placement and transfer of data is of utmost importance, especially when computing resources are physically allocated to countries located outside of the boundaries of the European Union.

Community legislation regarding the protection of personal data - already mentioned above - allows the transmission of data to a third country only if it provides an adequate level of protection (possibly with the consent of the

national authority that will evaluate the adequacy of the protection that the parties are preparing to ensure on the basis of negotiated agreements agreed, in accordance with current European legislation on the processing of personal data). The controls and formalities that must precede data transfer will be easier if there is a direct relationship between the user and the supplier or sub-supplier, resident outside the European Union. They will be more complex when multiple parties are involved in the provision of cloud computing services.

Another aspect that deserves attention is related to the possibility that large amount of data, provided by different owners with different interests, are treated by a limited number of multinational companies, with the possible risk of commingling and conflicts (the so-called big data).

8. Direct and indirect responsibility of suppliers and sub-contractors

The importance of regulating in detail the terms and conditions of the service is of utmost importance for the role that different actors play in the adoption of cloud computing services: service provider, providers of Internet access. Each of them need to receive adequate information and contractual guarantees, on the quality parameters of the service provided.

During the migration to cloud computing services, in fact, the user becomes completely dependent on the adequacy of the quality level of the suppliers. Each (even temporarily) unavailability or inefficiency of the services can have a significant negative impact and result not only in economic losses, but also in considerable damage to the user image. Accordingly, it is essential to introduce contractual clauses that provide for the payment of compensation, which describe, with the utmost precision, the performance expected by the user and to clarify how certain benefits are of crucial interest.

In general, providers of cloud computing services are similar to other service providers, whose obligations are essentially based on the Legislative Decree no. 70/2003 governing electronic commerce, in the transposition of the European Directive 2000/31/EC and, with regard to consumer protection, the Legislative Decree no. 206/2005, also involving the community. Also in general, specific measures must be taken into account as the provision of on-line services is a complex contractual operation, divided in two phases: the signing of the contract and subsequent execution. The contract, in fact, will evolve throughout the duration of the relationship and also after its termination. The supplier's obligations depend on the type of services offered and the activities carried out under the contract.

Liability arising from the provision of digital preservation must be provided by an analysis of many aspects that are reflected in the terms of contractual responsibilities placed in the hands of various actors: the service provider, any intermediaries (which contribute to the delivery of the final service), the role responsible for the preservation of data (for example, the legal entity which has been delegated parts of the process, including those relating to information storage in the cloud computing infrastructure). Storing data in different

geographical locations may have implications for all these actors of the applicable law in the event of a dispute between the data owner and the supplier, and in relation to specific national law governing data treatment, storage, and security. Therefore, in order to properly manage the contract with the cloud computing provider of services related to digital preservation it is crucial to apply the concept of "intellectual interoperability" between lawyers, archivists, and those who, as managers (of internal or external organizations), supervise the process adopted for the preservation of digital documents.

A good contract for the provision of cloud services (and digital preservation of documents) must therefore be the result of the application of the rules governing the liability of the supplier and the processes of safety and protection of the confidentiality of information, stating how and by whom data safety will be ensured. When establishing contractual provisions, the parties must also take into account all the obligations required by specific guidelines. For example, there are specific obligations that define the irresponsibility of senior roles with regard to the commission of crimes, through the provision of a suitable organizational model and the adoption of specific procedures for the optimization of the service, to be shared with the supplier. The contract will have to consider and provide for the application of international and ISO standards.

The contracts may have specific clauses to ensure confidentiality obligations, whose violation involves the payment of penalties. To prevent unauthorized or not allowed access it is also necessary to plan the use of both encryption, for data subject to transit operations, and adequate authentication systems, in order to guarantee with certainty the identity of those entitled to access data. The issue of cross-border data flows requires to set at least some minimum guarantees, in order to meet the requirements of Community law.

Data portability and interoperability of infrastructure with the computing resources of the users should be among the requirements to be accepted and respected by the supplier. To define any liability profiles of the entity that manages the data, it is necessary to clarify the exact legal nature of provider of cloud computing services. Even in the case of limited autonomy, the supplier should not be considered a controller but a processor, especially when the methods of data management are agreed between the user and the supplier through specific clauses.

A service provider is responsible for the management and its actions are limited to only certain data. In general, the provider does not have specific and appropriate skills to play a predominant role in their treatment. Like controllers, the provider maintains, however, autonomy and responsibility on traffic data related to the circulation of information, infrastructure or to the user's computing resources.

The division of responsibilities between the supplier and the user cannot be rigidly fixed. Existing models of cloud computing services can be easily integrated with each other, either when the supplier provides an integrated service, or when multiple providers compete to offer a complete service. Suffice it to say, for example, to the case where the provided service involves

processing and data management (storage, copying, transmission of data to third parties) where one has to distinguish between the operations of data processing carried out directly by the computer and those established by a human operator. Only in this case it is possible to recognize responsibility profiles, which affect other transactions related to the service provider.

Particular attention should be paid in the event that the supplier is entitled to honor the services contract with third parties, even if only for the management and the allocation of physical resources on which data resides. In this case, provision should be made in the contract specifications warranties relating to the sub-contract, requiring the supplier to notify this decision to the user.

The law applicable to the provision of cloud computing services is rooted to the physical place where the supplier is established. If the offender is a company based in the European Union this does not create any obstacle, as it applies to Community law. However, the problems on the legislation applicable in the event of a dispute between the service provider and the user can be included in more complex terms, the occurrence of situations in which the service provider interacts with other entities.

In a cloud computing infrastructure data are often stored in different data centers, which can be physically located in different countries. The service provider may also use third parties to exchange computational resources (for example, if the supplier does not have enough available capacity in terms of storage media and relies on others as well). Exchanges between several parties determine a continuous data flow, making it difficult to identify who handles them at any given time, nor their exact location. The user is then limited to access to the service and the provider will be in charge to retrieve his data. A plurality of contractual relationships also occur when the supplier provides a service which, in turn, is obtained from other suppliers, always in the cloud infrastructure.

Therefore, since different subjects may intervene in the management of the infrastructure it is necessary to regulate the cases where the supplier uses third-party vendors who do not reside in the European Union. There are many possible solutions ranging from (a) the use of Community clauses type between the user of the services and the sub-supplier, (b) the warrant issued by the user to the supplier, so that the latter directly enters into agreements with the sub-supplier, (c) the provision of specific contractual arrangements between the parties.

The signing a contract cannot, however, be sufficient for the user to be risk-free, since suppliers can contract certain activities (including management of physical resources that hold data) and can in turn be subject to corporate events (mergers and acquisitions) which lead to significant changes, such as, for example, the registered office and, consequently, the applicable regulations. In summary, even after signing a valid contract, it may be difficult for the user to request compliance with the obligations that have been covered, especially when the supplier does not reside in the same country.

9. Conclusions

The technological frontier moves quickly, changing lifestyles and assumptions previously considered absolute. In the case of cloud computing, the effects are still visible and not perceived. As citizens, we take for granted many of the services offered on Internet (home banking, reservation systems and online purchase of tickets, e-mail, remote data storage) without knowing that they rely on cloud infrastructure. More and more our society depends on these technologies.

The different speed of adjustment of the legal body of rules to the technological progress, increases the risk (but often the certainty) that the introduction of new services is not accompanied by a sound legislation that protects the interests of consumers but also of those who have invested in technology. Perhaps this is the novelty of the third millennium: a world in which the law must pursue reality and not vice-versa.

References

Bollier D., The promise and peril of big data, The Aspen Institute 2010.

Coleman N., Borrett M., Cloud security, who do you trust?, IBM 2010.

Data Protection Working Party – Art. 29, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, 2009.

DigitPA, Recommendations and proposals on the use of cloud computing in the public administration (Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione, in Italian), ver. 2.0, 2012.

ENISA, Certification in the EU Cloud Strategy, 2013.

ENISA, Priorities for research on current and emerging network technologies, 2012.

ENISA, Security and resilience in governmental clouds: Making an informed decision, 2011.

Enter the Cloud, Cloud survey 2013: The state of cloud computing in Italy (Cloud survey 2013: lo stato del cloud computing in Italia, in Italian), www.enterthecloud.it, 2013.

European CIO Association, Users recommendations from the European CIO Association for the success of the cloud computing in Europe, ARES 2012.

European Commission, Commission plans guide through global Internet policy labyrinth, ec.europa.eu/digital-agenda 2013.

European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard

to the processing of personal data and on the free movement of such data (COM(2012) 11 final), 2012.

European Commission, *A digital agenda for Europe* (*Un'agenda digitale per l'Europa*, in Italian), COM(2012) 245 def/2, 2010.

Flick C., Ambriola V., Data in the clouds: Legal aspects of cloud computing and application to the public administration (Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche, in Italian), Federalismi.it, 6, 2013.

Forum PA – Quaderni, PA on the cloud : G- Cloud: Gaining efficiency to innovate and reduce costs (La PA sulla nuvola: G-Cloud: innovare per guadagnare efficienza e ridurre i costi, in Italian), 2012.

Gantz. J.F., Minton S., Toncheva A., *Cloud computing's role in job creation*, IDC 2012.

Mantelero A., Outsourced computing processes and cloud computing: Management of personal and business data (Processi di outsourcing informatico e cloud computing: la gestione dei dati personali e aziendali, in Italian), Dir Inf. 2010, 673.

Schubert L., The Future of cloud computing. Opportunities for European cloud computing beyond 2010, Expert Group Report, 2009.

Biographies

Caterina Flick is a lawyer qualified in white collars and business, ITC law and cybercrime, privacy. Temporary professor of ITC law and privacy (University of Pisa, Siena, Lumsa of Rome and, since 2013, UTIU), she collaborates on research projects, participates to conferences. She is author of publications. She is consultant and lecturer at public authorities, including the Authority for the protection of personal data. Delegate at the FAO on behalf of IFWLC, she is also member of Committees for equal opportunities. Awarded in 2013 as *Excellent woman of Rome*.
email: c.flick@nmlex.it

Vincenzo Ambriola is full professor at the Department of Computer Science of the University of Pisa. Author of more than 100 scientific publications, his current research interests are in e-government, software engineering, programming languages.
email: ambriola@di.unipi.it