diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 28/10/2010

All'indirizzo http://www.diritto.it/docs/30421-cloud-computing-vs-jungle-of-data-protection-clauses

Autore: Marcoccio Gloria

Cloud computing vs jungle of data protection clauses

an opportunity to effectively standardize the measures required by law provisions on data protection & privacy

Cloud computing vs jungle of data protection clauses:

an opportunity to effectively standardize the measures required by law provisions on data protection & privacy

G. Marcoccio, October 2010

Foreword

What about cloud computing? First of all: it is about the reality, not a matter of the future, to be analyzed, estimated, assessed…. It is real. It is there. Probably we do not have complete awareness of this, but it is already present in most of our usual interactions with a computer or a communication device: being a part of a social network, surfing the web, purchasing a product via internet, accessing a web portal for business purposes, how many of these processes are already served by cloud computing? Many, many, and again many.
Our attention is required on the special nature of cloud computing, to be an undeniable and powerful catalyst to claim standard data protection measures, recognized and accepted by national legal frameworks.

A step back

As defined[1] by NIST, the U.S. Government's National Institute of Standards and Technology, "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*".
In other terms this means that the resources you access by your computer or communication device are the result of the interoperation and integration of hardware and software and communication resources, located everywhere in the world, managed by different providers, devoted to provide services to a variety of users.
Cloud computing is presently delivered via three different models, always reporting the NIST definitions:

> ***"Software as a Service (SaaS):*** *The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running.*
>
> ***Platform as a Service (PaaS):*** *The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework.*
>
> ***Infrastructure as a Service (IaaS):*** *The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them."*

Whatever is the delivery model, the big promise of cloud computing for the end users is to pay on demand basis for the use of computer/application resources. This is one of the reasons why cloud computing is

[1] http://csrc.nist.gov/groups/SNS/cloud-computing/

often compared with the public water or electricity resource provision: you pay water only when the tap is open, you pay electricity only when the switch is on.
Although this comparison does not properly match cloud computing (usually it's a two-way flow: from one side you get some resource, from the other side you provide something, like for example your personal data to be retained in a memory device…), on the other hand it effectively represents a self-evident fact: anybody understands that it is easier to purchase the centralized water provision service rather than to build and manage his/her own well.

Cloud computing initiatives and information security & privacy aspects

The legitimate expectation to lower costs and maintain/ increase quality and reliability of the services is driving many companies and public bodies in the direction of cloud computing: one of the main examples on this is given by the U.S. government, which is declared as "the world's largest consumer of information technology, spending over $76 billion annually on more than 10,000 different systems". The U.S. Federal Chief of Information Officer (CIO) issued in May 2010 a very interesting report "State of Public Sector Cloud Computing", in which are outlined, in a real pragmatic way details on deployment models, service models, and common characteristics of cloud computing and in general guidance to foster the adoption of cloud computing technologies.

Also on the European side, there are several initiatives along the direction of cloud computing strategies and implementations: one of the examples is given by the contribute of ENISA[2] with its valuable report "Cloud Computing: Benefits, Risks And Recommendations For Information Security" issued in November 2009.

But, as initially said, cloud computing with its benefits and risks is already a reality and its information security and privacy issues need to be addressed and solved soon. This is perfectly clear for the organization named Open Cloud Manifesto[3], aimed to establish "*a core set of principles to ensure that organizations will have freedom of choice, flexibility, and openness as they take advantage of cloud computing*". The Open Cloud Manifesto sets a reliable basis to encourage vendors to work towards open solutions and also to address, via technical standard, information security and privacy demands.

- Who can access to my business/personal data?
- What happens to data in the event of a disaster?
- What happens in the event of a security breach?
- And what about the implementations required by the privacy national regulations? Who is data controller? Who is data processor? What about limits and constraints on transfer of personal data abroad?
- Who is responsible for the implementation of the necessary security measures?

Without common international provisions on information security and privacy it seems very difficult to answer the above questions. We can image the jungle of contracts which would rule information security and privacy responsibilities and duties within a real cloud computing scenario.

[2] http://www.enisa.europa.eu/
[3] http://www.opencloudmanifesto.org/index.htm

It is difficult to claim harmonization and effective control with a multitude of contracts among several parties, customers, final users/subscribers, providers, vendors involved in cloud computing use, operation & maintenance, in a multi-national context of regulations.

However, cloud computing could be the strongest supporter of the cause of "privacy by design", at least to achieve technical rules, shared and agreed at international level.

Demands and steps ahead for the purpose of harmonization and standardization

The need for a greater and more effective harmonization of the national data protection & privacy laws is clearly an incontestable fact: in this sense it is essential to acknowledge the work already started by many Data Protection Authorities. In November 2009 the authorities from over 50 countries approved the "Madrid Resolution[4]" on international privacy standards, which constitutes the basis for the drawing up of a future universally binding agreement of the national privacy laws. The approved resolution includes a series of principles, rights and obligations that any privacy protection legal system must strive to achieve.

Same needs has been recently reinforced by Viviane Reding, vice-president of the European Commission and Commissioner for justice, fundamental rights and citizenship, in her speech during the Conference organized on 16 September 2010 by the Lisbon Council Brussels on "Unleashing the digital single market". She announced, among other things, she would make a proposal for the future revision of the present European Data Protection Directive. *"In order to encourage new technologies in an environment in which consumers know their rights, different solutions could be found such as "privacy by design". Data protection compliance should be embedded throughout the entire life cycle of technologies and procedures…The Digital Single Market should also be a cyber crime-safe environment, and for this purpose the Commission will propose criminal sanctions against people responsible for cyber attacks"*.

Everything seems to be going in the right direction for the purpose of convergence and harmonization: a path not easy and certainly not short due to the many and varied needs to comply with several national legislative frameworks, often very different one from each other.

But realities as cloud computing, require more rapid and effective interventions, in line with consumers expectations and the needs of companies to make their business. It is reasonable to expect that such complex issues will be decomposed in feasible subsequent steps, as for example: aggregating consensus toward initiatives as the Open Cloud Manifesto, finalized to carry out a set of technical/procedural requirements to be met, which also includes the concepts of "privacy by design", and a greater coordination between the privacy authorities, which is believed they have an increasingly important role in the process of standardization and internationalization, about what operatively regulates information security and privacy measures.

4

http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf