JICLT
Journal of International Commercial Law and Technology
Vol. 10, No.1 (2015)

SOME LEGAL ASPECTS OF CLOUD COMPUTING CONTRACTS

Carlos A. Rohrmann & Juliana Falci Sousa Rocha Cunha

Abstract: Cloud computing is a current reality in technology that is being widely adopted by large companies. This study discusses cloud computing and information security. It also includes some of the advantages and risks, models of system and service adopted, as well as key services offered by the providers of cloud computing. It also addresses the legal issues of cloud computing contracts, with a focus on the contracting parties, on their goal and main clauses that must be addressed in this atypical contract, among them the integrity and confidentiality of data plus information requirements for supplying information and the purpose of the content stored in the case of a breach of contract.

1. Introduction

Currently it is very difficult for organizations to survive without the support of information technology, which enables a great improvement of business competitiveness.

With the growth of internet speed, business learned the need for a more quick and efficient interaction with clients. So, companies started to focus on their core business, leaving other activities to third parties. Cloud computing is a good tool for companies to accomplish such a goal.

At this point in time, cloud computing is widely used by big companies. It offers more advantages than disadvantages to companies, allowing them greater productivity, great data processing power and cuts desk costs.

In addition, cloud computing also allows IT companies to store and process their data remotely. Data can be retrieved anytime and anywhere through simple devices such as smartphones.

There are several services offered by the cloud providers, such as the storage of files, backups, provision and management, and software updating and service support.

However, in order to assure the security of the information, it is important that data is not accessed by third parties, including competitors, government and non-allowed users.

Thus, regarding the security of information, it is important that the service provider pays strict attention to client identification, to the use of encryption and the security of the whole infrastructure.

In order to maintain the legal certainty of the stored content it is essential to have a comprehensive business contract between the provider that offers the service of cloud computing and the client who uses the service.

2. Cloud computing and the information security

2.1 Concept

Cloud computing and its concept have evolved significantly in recent years.

Initially, data was stored inside the company's own computer systems, with no possibility of external storage neither remote access.

Subsequently, data began to be stored on a computer of external company, outside the corporate environment, the so-called data centers - often outsourced services.

They had several servers, which enabled the storage of large volumes of data, including the data of more than one company.

Nowadays, the storage service has evolved considerably, allowing us to store important corporate data in the clouds. Thus, authorized corporate users access information easily from any location, at any time, via mobile devices.

Large organizations or large regional providers, such as Google, Amazon, Microsoft and HP, offer those services. However, the growing fear for leakage and unauthorized data access is noticeable.

Many theorists claim as the most relevant definition of cloud computing the one issued by the National Institute of Standards and Technology-NIST:

> *Cloud computing is a model for enabling 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*. (Mell & Grance, 2011, p. 2)

Finally, cloud computing is a service offered by a company to natural persons or client companies upon an atypical contract, which has as its object, services such as storage, processing and backup content, providing customized applications and others on the server contractor, allowing the client or other authorized person to have secure access from anywhere, anytime, through any mobile device.

2.2 Some advantages and risks of cloud computing

2.2.1 Advantages

There are many advantages of cloud computing, but biggest advantage is the fact that there is no need to worry about complex tasks of indexing data, and thus the client company can focus on its core business and consequently be more competitive, efficient and profitable.

The benefits from the enormous processing power that it is offered by the provider of cloud computing services are growing. The client company does not have to invest a large amount of capital in hardware and software, maintenance and upgrade, neither in the management of information technology.

Consequently, another important point is cost reduction, which allows the allocation of capital in the core business.

Cloud computing relies mostly on the internet, which is already available to most large companies.

It is also important to mention the ability to optimize data processing. In most cases large companies fail to utilize much of their IT during off-peak times.

In this way, the underutilized resources are offered to another organization that is demanding on that moment, without delays to other companies. Thus, the service provider can optimize the resources available from one company to another, depending on the demand that occurs at that moment.

Cloud computing also enables the employees of the client company to use the information and data anywhere in the world, at any time and on any platform (mobile or not). In the past it was common to find enterprise environments with their own providers. By accessing cloud computing, the collaborative work is strengthened, and it allows the employees of various areas of the organization to access and modify documents 24 hours a day, 7 days a week, regardless of where they are.

Seasonal or cyclical businesses that do not constantly need large processing capacity can hire the services of cloud computing for a specific period. According to their needs it can be done without major investments in personal computing, and without hiring an overestimated computer service.

Regarding data safety, the risk of data loss is reduced with cloud computing service, since there are many processors at work and there is a specific structure of hardware to perform periodic backups. The service provider can also be held responsible for the loss of data. However, this issue must be properly addressed in the agreement. In addition, the traffic of peripheral equipment with business information (e.g. thumb drives), some of them with possible highly confidential content. This could jeopardize the whole business strategies, but such a risk is reduced with the implementation of cloud computing.

Another advantage of cloud computing is the energy efficiency related to the companies that adopt this system. The amount of energy expended by a cloud computing service (which is a large center of storage and data processing) is lower than the amount expended by several centers of traditional data processing. The cloud computing servers have energy efficiency programs and seek to consume clean energy or are installed in locations where the temperature is low, to reduce the use of chiller machines.

Last but not least, the availability must be addressed. As to the cloud computing hardware, if a failure occurs, the machine is automatically relocated in a matter of seconds, which makes the impact (downtime) imperceptible – there is no harm to the company core activities.

2.2.2 Risks

There are some disadvantages in the use of cloud computing, such as the possibility of information leakage. Therefore, it is essential that the staff responsible for contracting the cloud computing service performs detailed analysis, seeking to maximize the guarantees offered by the service provider.

Companies interested in cloud computing services should keep in mind that they might not have exclusive control over the data stored in the cloud.

There is also the risk of loss of data and sensitive information by the contracting company, which can have directly impact on the company results. Therefore, it is important to know the backup plan available by the service provider, but many providers refuse to inform it, stating that it is confidential information.

Another critical point of any service cloud computing is data security (including privacy), especially in these days with so many issues relating to leakage and theft of contents being addressed.

In terms of information security, many topics can be addressed, among which, the integrity and updating of systems, protection of stored information and information in transit, besides data recovery procedures against disasters.

These issues can be addressed in the cloud computing contract as well as in the Service Level Agreement (SLA), which should appear as an attachment of the contract.

Regarding the reliability of the stored content it is important to emphasize that the provider may be required, by court order, to make such content available or to disclose it even if the contract has a specific clause of reliability. Thus, it is important to make the client company aware of the data protection legislation of the countries where the content is processed and stored.

The location of the servers that store and process the contents of the client company shall also be verified, because such data may be stored or processed in one or more locations, which can later cause problems for the client company.

The actual availability of the internet is also important. Due to the growth of internet usage and the migration of many computing resources to the cloud, flaws that preclude access to part or all of the content stored in the cloud may occur. Unfortunately interruptions have been more than desired. It generates damages to the client company, which has a direct impact on its revenues.

Finally, cloud computing has evolved considerably, including bringing new services to client companies and natural persons. Along with this evolution many strengths and opportunities for improvement have emerged, which should be carefully evaluated by potential client companies which want to use cloud computing service.

2.3 Deployment Models

The basic deployment models are: private cloud, public cloud, hybrid cloud and community cloud.

Private cloud (or internal cloud), is typically the first step of a large company. It is one whose infrastructure is acquired and managed by the client company itself or by a third party, but operated exclusively for the benefit of that client company (exclusive use of the company and authorized users).This type of cloud is costly for developing, deploying and for maintenance.This cloud can be hosted by the company itself or by a service provider.

Despite the minimal dependence of the company that uses this model with respect to other companies, the service will be subjected to the public internet service, since the internet is necessary for accessing the cloud. Private cloud presents a main advantage in higher security control.

A community cloud, usually the first step undertaken by small and medium businesses, is shared by several companies with common principles and interests, as, for example, security requirements and policy. Such a service may be administered by any organization that is a part of a consortium.

The hybrid cloud has its structure composed of more than one type of cloud. The private cloud, for example, may have its resources increased from the resources available in the public cloud. In this case the desired level of service can be maintained even if there are rapid changes in the resource needs of the client.

2.4 Models of Service

As for service models (or business), researchers emphasize three main models of cloud computing service: Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS). (Valenzuela&Montoya, 2012, p. 31-32)

It is noticeable that each service model entails different legal responsibilities by the service provider and regarding the client.

Thus, it is important that those provisions must be included in a computing service contract, and all information related to the ability of the service should also be included in this document.

It is also noticeable that there is a trend to create new models in the future, according to the growth of the services offered by cloud providers.

2.5 The Services provided by cloud computing companies

The main services offered by cloud computing companies are the storage and processing of files, backups and the availability of software.

As to data storage cloud service providers ensure that one can store any type of files such as text, spreadsheets, music files, photos, and presentations, among others, assuring reliably, full availability and low cost.

Besides the storage, management and the updating of applications are also some services offered by cloud computing providers. They also allow the employees of the contracting company to access software and information they need. This avoids unnecessary expenditures on the acquisition and continuous updating of applications used by company employees.

There are also cloud computing providers who are willing to develop applications accordingly to the needs of the contracted third parties. This service is tied to the upgrade, maintenance and management of the customized application which will be available in the cloud.

Another service offered is the reliability of the data and information available in the cloud. Undoubtedly, no cloud computing provider can guarantee 100% reliability, but can reduce the instability of the information system. Goals of service stability and sanctions, in case the indicator will not be achieved, should be addressed in the terms of the service agreement.

Moreover, cloud computing providers usually offer support by their own technical staff. With cloud computing, technology employees of the client company tend to be reduced. It is important that the service provider offers available support, over telephone or physically, aiming to remedy any operational problems or questions, especially those that cannot be solved by the internal IT staff of the client company.

Thus, it is noticeable that there are many possibilities of combination of services to be contracted, and, of course, other customized services may also be developed. The optimal configuration of services varies from organization to organization and must be analyzed in detail.

The market for cloud computing is expanding rapidly and offers great business opportunities. Accordingly, companies wishing to make use of this technology should consider what services they really need. In the manner indicated, they will enjoy those that offer more advantages to the various types of business enterprises.

3. The Contract of Cloud Computing

The relationship between cloud providers and their customers generate wealth for society, but can also generate conflicts, mainly because it involves a service of technology and information security.

Regarding large enterprises, focus of this study, a clear and well-written contract is more important due to the great amount of data and sensitive information to be managed. Such data is related to customers and employees information. Generally, when the customer is a large organization, the service contract can be customized, aiming to supply its specific goals and objectives, which does not occur when the customer is a natural person or a small business. Such clients are subject only to the provision of a standard service, without any of the adaptations, which will be detailed later.

Moreover, the contracts signed by large corporations, as all types of contracts, requires the presence of basic details, as the names of contracting parties and the object of the service to be contracted. However, a previous detailed analysis of the important requirements for both contracting parties must be done. For example, some items are to be discussed previously: the privacy of information, interruption in service provision and data security.

Generally, bigger users, particularly from regulated industries, try to negotiate more. Some even require contracts to be on their standard IT services or outsourcing terms, on a ‘take it or leave it’ basis.

As to the will externalized in a contract by the customer:

> *Quanto maior o afluxo constante de novas e mais sofisticadas tecnologias, tanto menor será o poder de reflexão e a possibilidade de se externar uma vontade racional, pois esta será apenas uma vontade distorcida pela pressão psicológica, expressando, por consequência, muito menor do que deveria ser, pois incapaz de externizar a verdadeira liberdade contratual*. (Rohrmann & Machado e Campos, 2009, p. 70).

This is easily seen in consumer contracting, where in most cases, consumers sign contracts online without analyzing them in detail or even without reading them. They do so because of the need to access, for example, a particular content or application. Some of them explain that they do not understand contracts in general, even a contract involving technical terms related to technology. Consumers mostly sign electronic service contracts without reading the terms.

3.1 Contractual Parties

With regard to the parties that constitute the contract of cloud computing, they are identified as the supplier of the service or Cloud Services Provider (CSP) and the client company (or a natural person) that will use the cloud storage.

The client is interested in the services offered by the service provider and is willing to sign the contract for cloud computing, aiming to benefit from the service upon payment (free service can also be provided).

The client may be a natural person or a legal entity, which directly influences the possibility of discussion and negotiation of the contractual clauses which are being studied at this point in the process.

Large companies, including banks and public corporations have more power to discuss such clauses. This way, they are able to customize, at least in part, the contract of cloud computing.

However, contract customization is difficult when it refers to a natural person or small and medium-sized companies. They generally enter into contract without modification, i.e. an adhesion contract.

It is noteworthy that this type of agreement can be celebrated online. It will probably be difficult to find few suppliers willing to negotiate the terms, even if the other party is a great company.

Usually a cloud service provider is a legal entity. However, a natural individual can also perform the task of a cloud provider, since they have the infrastructure and other necessary resources. Nevertheless, in the survey conducted for the preparation of this study, individual cloud providers were not found worldwide. Generally cloud computing providers are large multinational companies.

3.2 Object of the Contract

In cloud computing contracts the detailing of the object must be written accordingly to the service model to be adopted. For example, the object of the provision of application (SaaS) is different from that one detailing only the provision of the infrastructure (IaaS).

Anyway, it is very important to emphasize the significance of the description of the object of the contract.

The description and the scope of the object of the contract are, in practical terms, determinants on the technical scope of the service to be provided and the content of the obligations of the parties.

Therefore, clients that will use the service should pay attention not only to their needs, but also to the terms of the service contract. Such a document regulates the relationship between the parties and will clarify the scope of the contracted service in the case of future litigation.

3.3 Some more relevant contractual clauses

To use a program or an online service in the online world, the agreement terms of the supplier must be accepted. This also occurs with cloud computing, in which the client must agree to the terms of the service agreement submitted by the supplier.

Usually when clients of cloud computing services are large companies, some terms are widely discussed and negotiated. However, for small and medium sized businesses and consumers, service providers offer their service as packages and standard contracts. For example, when a consumer registers in an information store service in the cloud, such as Mega, she clicks accepting the terms of service and there is no room for changing any of the contract clauses.

Whatever the type of contract of cloud computing, such contract should always be as clear as possible. It should also be interpreted in accordance with the intention of both parties, with preference to consumer protecting policies.

In addition to the various clauses that can be part of the cloud computing contract, such contract should also be drafted considering the client's business, the type of customer (industry or government, individuals or companies; small, medium or large corporations, for example). The contract also should be suited to different models (public cloud, private, hybrid or community) and service (IaaS, PaaS and SaaS).

The European Network and Information Security Agency ENISA (2009), a center of excellence in network security and EU information, identified some issues that must be addressed in terms of cloud computing contracts: data protection, availability and completeness, minimum standards of security, confidentiality, intellectual property, professional negligence and subcontracting and exchange control services.

Therefore, there are many contract terms, and some are more relevant in certain models of service and business than in others. This text addresses some clauses considered most relevant in the cloud computing contracting.

Some contracts are not denominated Cloud Computing Contracts, but Terms of Use (usually between natural persons or small businesses), Terms and Conditions, or even are part of the SLA.

There is no doubt that the typical contract clauses must be included in any contract under study, as the complete qualification of the parties and their legal representatives, place of celebration, duration and renewal. Other important clauses are price and terms of payment (date, form of payment, bank transfer, implications of non-payment of monthly fees, late payment fees, suspension and cancellation of services).

However, some of the agreements refer to the Privacy Policy, the SLA or the Policy for Use of cloud provider, which form a part of the contract. Some contracts have focused on consumers and small-medium enterprises, and refer to the Terms of Use, the SLA, the Privacy Policy and the Acceptable Use Policy.

As for software, the contract must regulate its support, maintenance and updating, in addition to the responsibilities of the parties. In contracts involving large corporations, usually software may be developed as a customized computer program.

The provision of service availability is especially important for the enterprise customer. Usually performance indices according to the efficiency of the provider are established around 97% or 99%. Furthermore, some providers contractually describe exceptional situations which might not provide the service, such as power outages, fortuitous events or public internet service interruption.

Schedules for performing maintenance can be provided in a clause of availability, as well as improvement and updates by the cloud computing provider, thereby generating the least possible impact on the client company activities.

The integrity of the content regarding storage and preservation is linked to the liability of the cloud service provider.

Many service providers do not allow the inclusion of a contractual provision regarding security against loss of data, especially those who provide free cloud services. In this case, at most they are committed to make the "best effort" to maintain the integrity of information in the cloud, which means that if any loss occurs they are not held accountable.

Eventually server failures take place in the cloud, even though the service providers might not confirm such events. One way to minimize the impact of failures is to guarantee contractually that the content of the cloud will be stored in different virtual machines, thus reducing the risk of loss of data.

The protection and privacy of content stored in the cloud should be mandatory in all contracts for cloud computing, because if there is no contractual provision in this regard, theoretically the supplier could even sell third parties data (of course depending on the legal regulation of the jurisdiction regarding personal data).

In some cases, data protection is subject to specific and detailed document that is part of the cloud computing contract, which reinforces its relevance.

To reinforce the privacy of the data stored and processed in the cloud, the client company can contractually require the service provider to record the activities (logs made with date and time) during a specified period. This policy will enable a rapid and accurate response in case of an incident, because the logs can be available easily. However, those logs should never be changed by any party. It can also be agreed that the service provider will conduct random testing on the availability of logs and send the result to the other party.

It can also be discussed between the parties to provide a clause stating that the client company will be notified of legal and administrative requirements for content delivery; in this clause it would be stated what was available, when and to what legal authority. Exception should be made in cases where the legal authority prohibits such communication is performed, for example, when it is necessary to maintain the confidentiality of a criminal investigation.

Another important clause is the confidentiality, whereas employees and subcontractors of the cloud provider may have access to sensitive client company information, due to the performance of their

function (maintenance, administrative, technical and other). Generally providers seek to make the other party aware of this issue. Some providers demand that contracted staff and outsourced service personnel sign an agreement regarding this.

It is important to make it clear that the reliability of a cloud computing contract is not restricted only to the data and information stored in the cloud. For example, it should cover documents exchanged between the provider and the client company, conversations and understandings as well as the business model adopted.

Furthermore, the contracting parties should discuss the liability of the service provider for any willful or negligent action that should be undertaken by its employees or subcontractors, which could be contrary to the contractual confidentiality clause.

It is important to negotiate the possibility of the cloud computing provider to contract (or not) subcontractors, what should be foreseen in the service contract, and to what terms third parties would be bound by the original agreement.

It may be agreed, for example, that service providers will only be allowed to contract subcontractors eventually and under express approval of the other party. In this case, safety conditions must also be applicable to subcontractors. Some companies require that they must be informed about the identity of the subcontractors' employees and the changes in the staff; this should be a provision of the service contract.

Another important issue to be handled by the contracting parties is the law applicable to the contract, since the data can be stored in other countries.

The law applicable to this type of contract in most cases is related to a jurisdiction which may be the jurisdiction in which the provider has its principal place of business.

However, the acceptance of a clause with such applicable legislation by the cloud provider is difficult, since the vast majority of providers have infrastructure in several countries, according to the low cost of maintenance, cost and availability of energy and technological resources, which make it difficult to customize the service.

The contractors must also choose a territorial jurisdiction that will be responsible for applying the law elected by the parties. In Brazil, when choosing the national law, the parties also elect the Brazilian jurisdiction to deal with conflicts. In this case what can be changed is the court, and, generally cloud providers elect São Paulo.

Being elected arbitration for dispute resolution, the parties should choose the regulation and the jurisdiction that will be applied.

In some countries there is no specific legislation related to cloud computing. Other jurisdictions such as the European Union have enacted legislation regarding the issue. In the United States, for example, there is a legislation that permits the government to have access to any information stored and processed in the country, for reasons of national security.

So, it is prudent to discuss widely the question of legislation on cloud computing. This may occur through international bodies, since it has an impact all countries and the international law.

Protecting copyright, trademarks and trade secrets stored in the cloud is also a huge issue that is beyond the scope of this article.

As for the software developed and marketed by third parties used in the cloud, it is important that the contract for cloud computing specifies which contractor will be responsible for licensing, as well as for its update.

Normally the contracting companies share the cloud environment with other client companies of the provider. In these cases it is important to use and contract the encryption of data as well as the encryption program to be used (preferably with international certification). Another issue to be discussed is the separation of data, since some IT experts say that if such activity is not performed eventually there may be impact on access and recovery of encrypted data.

As for the providers monitoring of the cloud, many clients fear that by accomplishing it the provider may access restricted content and disclose both the content stored in the cloud and the result of monitoring. In contrast, providers ensure that monitoring occurs only in order to arrange the cloud properly to the client company needs; in other words: auditing storage space and processing regarding the size, the verification of time response and the suitability of bandwidth, among other details should be required. Therefore, the contracting parties should establish whether the monitoring will be admitted in the contract, and if so, what type of monitoring will be authorized.

Another issue that should be discussed by the contracting parties is the retrieval of content in the event of tampering or deletion. Will the provider of cloud computing backup data stored at what rate?

Another important issue that must be addressed in the contract under analysis is the security of information to be transferred, i.e. the security of the content that will be transferred between the parties over the internet. This concern is due to the fact that large providers of cloud computing services have multiple data centers and develop their own safety nets.

There may contractually be set an audit, for example, with respect to the integrity of the stored content, to the security of the contents to be transferred, to the performance of the service and to the safety of the cloud provider's infrastructure. This audit should be performed at the direct service provider and at the subcontractors. However, if there is no contractual provision to allow it, the service provider is not obliged to consent to it. It is noteworthy that the audits are difficult to carry out, given the large number of servers, the various locations where they meet, besides the high cost involved in such activity, which, however, does not diminish the importance of the audits.

The auditing companies may be stipulated in the contract of cloud computing, as well as the frequency of the audits. Ideally, the audit firm should be an independent one, and if the data is to be stored in different countries, the best firm to conduct the audit would be an international service company. This company should be specialized in information security audit, data processing and cloud computing. Regarding the audit report it can be stipulated that it may be sent to one or both contracting parties.

It can be predicted that the provider will have a deadline to act on correcting problems found by the audit.

It can be reason for the termination of the contract, as well as penalties against the provider, if the vulnerability or flaw is not corrected in a timely manner.

And as to whether the supplier ceases to exist or undergo a merger or acquisition?

When it comes to merger or acquisition, often the new company has no interest in keeping some of the customers or the strategies previously established. Any of these situations may lead to improper disposal of customer content or even service interruption. Therefore, it should be stipulated contractually that the new provider will comply with the contractual terms agreed during the contract negotiation. It can also be agreed that the provider will notify the client company on the operation performed (e.g. merger and bankruptcy, among others), and may terminate the contract.

Another issue that must be included in the cloud computing service contract is related to the preservation of the content at the end of the validity period of the contract. Will the provider hold the content or must it be returned to the customer? Will it be sent or made available to another provider indicated by the provider or by the customer? In what format should it be done? Will the provider delete the content safely (including backup)?

When it refers to a company that deals with ultra-sensitive data, such as financial and medical institutions, it can be defined that the client company (or a third party indicated by it) will audit the provider when the contract expires, in order to verify if all company data were actually deleted.

The time of preservation of the content by the provider can be radically reduced if there occurs breach of the contract or breach of any document that is part of it, as the Usage Policy. With respect to non-payment of the contracted service for a certain period, it is common the provider does not accept the task of keeping the agreement, as well as the storage of the content in the cloud.

What about a content infringement, invasion or attempt of invasion? It is important to discuss a clause that foresees that the supplier shall communicate the fact to the client company, as well as the measures taken and what content was accessed.

It is also important to foresee penalties for breach of contract, such as providing information to unauthorized persons, not providing the contracted service capacity, as well as a contingency plan to be adopted by the service provider. Example of penalty is a financial compensation for the damage caused. Regarding secrets, for example, attention should be paid to the importance of its protection, even when it is available in the cloud.

With respect to changes made to contracts, it was found that in a contract where the client party is a small-medium sized company or a natural person, usually unilateral changes are conceded as valid by the provider, which the client undertakes automatically.

With reference to large companies, as they have greater bargaining power, it may be agreed that any contractual changes must have the prior written consent of both parties.

Contracts generally exempt providers of cloud computing of any kind of accountability, which can be negotiated mainly by large clients, such as financial institutions and government.

Cloud computing contracts stipulate the basic features of the service that will be available, as the size of memory for storage. Generally the monitoring of services is performed by cloud provider and such monitoring is made available to the customer.

As to changes in the service offered to a natural person or a small business, such changes happen without the full knowledge of such natural person or small business. In these cases, as a rule, the client is aware of the change if the new term of service is available in the provider web page or if there is a notification by email or other means by the service provider, which rarely happens.

However, as to big client companies, this issue is largely negotiated between the parties and is subject of a contractual provision. In some contracts changes with specific deadlines for advanced notification by the provider are established. There are also contracts that admit their termination if the

change made by the cloud computing provider impacts substantially on the service offered. In such cases, the parties must agree on a time that allows the client to migrate to another place

A great part of the cloud computing contracts deals with the possibility of suspension, resolution, and termination. But any contractual termination of the cloud computing service, especially the case of a big client company, must be well planned. When the client company takes the initiative of ending the contract service, it must first hire another service provider or have hardware and software to absorb the service that was previously provided by the third party.

Finally, in certain contracts for cloud computing service there is an item relating to definitions. This item clarifies the concepts of specific words that have been used throughout the document, which helps its interpretation by contracting parties, judges and arbitrators.

Thus, there are various issues to be negotiated between the parties, but the interpretation of contractual clauses should be carried out in accordance with good faith and the intention of the parties involved.

4. Conclusions

The digital world is a reality that affects the society as a whole, individuals or legal entities. Initially cloud computing may have been more widespread among individuals, however, now its diffusion into business is greatly increasing.

Therefore, it is essential that professionals in information technology and the legal department of large companies are technically prepared to negotiate and enter into comprehensive contracts providing cloud computing.

In such context it is necessary to properly understand the services and deployment models available in the market, as well as the various solutions offered by companies providing this cloud computing services, which usually have a global scope.

Thus, contracts for the supply of the cloud computing services shall stipulate clauses that meet the interests of both parties. For example, not only security, integrity and reliability of the information stored and processed in the cloud, but also issues regarding intellectual property and data encryption.

As addressed in this brief study, there are many legal issues to be discussed by the parties in this new environment such as the right to remove personal data stored in the clouds, accordingly to the right to be forgotten.

Finally, cloud computing is an increasing IT model with new advantages for companies that hire that service. These advantages are the ability to focus resources and energy on their core business, cost savings, high availability of data storage and increased productivity and profitability. But it is important to address the potential new legal impacts of cloud computing. It is also important to write contracts of service where duties and obligations of each party are clearly understood, thus avoiding subsequent drawbacks, such as loss of strategic and sensitive information to competitors.

* * * * *

Reference List

European Network and Information Security Agency.(2009). *Computación em nube*: *Beneficios, riesgos y recomendaciones para laseguridad de lainformación.* União Europeia: ENISA.

Mell, P. & Grance, T. (2011). *The NIST definition of cloud computing*: *Recommendations of the National Institute of Standards and Technol*ogy. Retrieved May 5, 2014 from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Rohrmann, C. A. & Machado e Campos, M. (2009). Oscontratoseletrônicos: Um estudo histórico-comparativo dos direitos brasileiro e europeu. *Revista da Faculdade de Direito Milton Campos,* 18, 23-76).

Valenzuela, D. P. & Montoya, J. D. B. (2012). *Aspectos legales de lacomputación em lanube*. Bogotá: Universidade Externado de Colombia.

Cite as: Rohrmann, C.A. & Cunha, J.F.S.R., Some Legal Aspects of Cloud Computing Contracts. *Journal of International Commercial Law and Technology,* Vol.10 No.1 (May, 2015)