Article **Journal-Law and Economy**
December, 2018 Vol.2 No.3 19-31

Legal and practical aspects of the use and development of cloud computing

Aspectos legales y prácticos del uso y desarrollo de la computación en nube

SUAREZ-JASSO, Elsa*†, OTERO-ESCOBAR, Alma Delia, MÉNDEZ-ANOTA, Mayra Minerva and MARTÍNEZ-HERRERA, Brenda Marina

Universidad Veracruzana

ID 1st Autor: *Elsa, Suarez-Jasso* / **ORC ID**: 0000-0002-7341-1068

ID 1st Coautor: *Alma Delia, Otero-Escobar* / **ORC ID:** 0000-0001-9266-6587, **CVU CONACYT ID:** 203484

ID 2nd Coautor: *Mayra Minerva, Méndez-Anota* **/ CVU CONACYT ID:** 314242

ID 3rd Coautor: *Brenda Marina, Martínez-Herrera*

Received August 15, 2018; Accepted November 22, 2018

Abstract

Cloud computing has now proliferated in an extraordinary way in various work, professional and educational fields. In Mexico efforts have been made to cover the legal aspects involved in the use of such an important service, trying to solve the existing gaps, since the advancement of technology has exceeded the time of legislation of the same. It is noteworthy that the legislation regarding cloud computing, not only includes the Mexican norms, but also the corresponding international norms ones according to the location of the service provider. The objective of this research is to identify the legal aspects of cloud computing based on the generalities that identify its use and application in current organizations. It is a documentary and descriptive investigation and its main contribution prevails in the compilation, interpretation of the legal aspects of cloud computing applied to a real case.

Cloud computing, Legislation, Technology

Resumen

La computación en la nube actualmente se ha proliferado de manera extraordinaria en diversos ámbitos laborales, profesionales y educativos. En México se han hecho esfuerzos por cubrir los aspectos legales que implica el uso de tan importante servicio, tratando de solventar los vacíos existentes, ya que el avance de la tecnología ha rebasado el tiempo de legislación de las mismas. Es de resaltar que la legislación respecto a la computación en la nube, no solo incluye las normas mexicanas, sino también las normas internacionales correspondientes de acuerdo a la ubicación del proveedor de servicios. El objetivo de esta investigación es identificar los aspectos legales de la computación en la nube partiendo de las generalidades que identifican su uso y aplicación en las organizaciones actuales. Se trata de una investigación documental y descriptiva y su principal contribución prevalece en la recopilación, interpretación de los aspectos legales del *cloud computing* aplicados a un caso real.

Computación en Nube, Legislación, Tecnología

Citation: SUAREZ-JASSO, Elsa, OTERO-ESCOBAR, Alma Delia, MÉNDEZ-ANOTA, Mayra Minerva and MARTÍNEZ-HERRERA, Brenda Marina. Legal and practical aspects of the use and development of cloud computing. Journal-Law and Economy. 2018. 2-3: 19-31

* Correspondence to Author (email: elsuajas@uv.mx)
† Researcher contributing as first author.

Introduction

The paradigm of the digital era is the framework of *cloud computing*. This is a term that, now and several years ago, is read and heard everywhere: in educational, technological, business, government, social networks, journals, research, innovation, among others, both in the national sphere and in international.

This article is presented as an analysis of the concept and legal uses of cloud computing. The legal situation is analyzed passing through different stages that go from the concept, the providers, services that offer, models of services of the cloud computing, advantages and disadvantages, until arriving precisely at the revision of laws, regarding the security measures and legal to be adopted in relation to this technological service, applicable when receiving / giving the aforementioned service. Finally, reference is made to some practical cases of companies to determine how their use and implementation is carried out.

This article aims to achieve the following specific objectives:

– Identify the provider, as well as the user.
– Understand the development and operation of cloud computing.
– Publicize the legal framework in which the confidentiality of cloud computing is developed and developed.
– Identify the risks of data security and privacy.
– Understand the legal commitment to the new scenario that cloud computing puts before the user and the provider.

Basic generalities and techniques of cloud computing

Cloud computing is a beneficial technological trend if it is used correctly, otherwise it can lead to legal problems. Thus, the National Institute of Standards and Technology has defined it as a model that allows a convenient access, in demand of the network, to a shared set of computer resources (Mell & Grance, 2009). It has also defined cloud computing as "it is a service that works through the Internet that allows users to store information of any kind: music, videos, in general and can have them hosted on dedicated servers, in teams that always they remain on 24 hours a day and 365 days a year " (Martínez & Gutiérrez, 2013).

The company (2017) defines in a simple way the cloud computing as: "A technology that allows remote access to software, file storage and data processing through the Internet, thus being an alternative to running on a personal computer or local server. In the cloud model, there is no need to install applications locally on computers ".

Cloud Computing offers individuals and businesses a large capacity and variety of computing resources with good maintenance, insurance, easy access and on demand.

Within the characteristics of cloud computing can be listed:

– Payment according to consumption, that is, paying only the services that are used.
– Ubiquitous access, allowing the use of services anywhere, anytime, provided that the internet service and the equipment for access are available.
– Availability of resources, that is, they can be used by different users or at the same time if required.
– Flexibility, in this way saves time and facilitate online procedures.
– Controlled service, the services that the user consumes are measured for control purposes.

Cloud computing works through various service models, which are related to hardware, platform and applications, then Table 1 describes these services:

SaaS Software as a Service	**PaaS** Platform as a Service	**IaaS** Infrastructure as a Service
Organizations buy or develop their own business applications and run and manage in their own infrastructure. Security is controlled by the service provider, the subscriber of the service only has access to limited administrative privileges.	It is delivered on demand, deploying in the software and hardware that is needed. Subscribers have partial control of the applications and environment configuration. Easy access to application programming.	The provider provides the technological means necessary for the client to make use of both the hardware and software of the requested service. It represents a saving in the acquisition of resources by offering them in a virtual way, being their use efficient and on demand.

Table 1 Model of cloud computing services
Source: Self Made

ISSN: 2524-2113

Figure 1 shows the three cloud computing services with some examples:

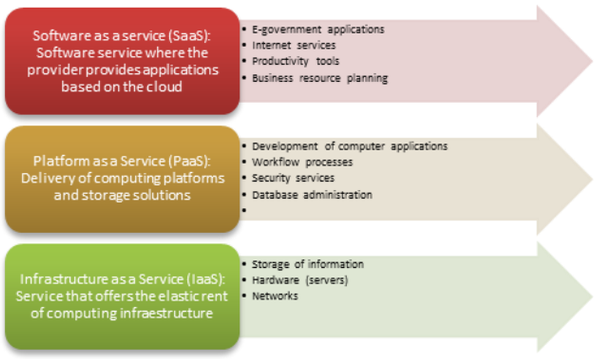


Figure 1 Cloud computing services
Source: (GSA, 2010)

Table 2 shows several models of cloud computing, according to the availability and access to data in the business environment.

Public	Private	Hybrid	Community
Everyone has access to information.	The information is only available for one unit.	Different dependencies share information between them.	Set of dependencies share resources for a single benefit.

Table 2 Cloud computing models
Source: Self Made

Regardless of the services in general and the models of cloud computing, the user always seeks the security that the service can provide, being this a relevant point for the design and implementation when solving cases of cloud computing.

Currently, the outsourcing of services has made it essential to increase and re-formulate security and legal measures, in order to ensure that the management of information in the cloud is real and completely secure. One of the main concerns addressed in the subject of security and reliability of information is the loss of it, which can cause serious economic and legal problems. To be able to provide cloud computing services it is important to have a provider, responsible and interested to safeguard the information, in such a way that guarantees a good service without risks that lead to the loss of information or damage to any of its critical systems.

Thus, it can be said that within the basic security aspects that must be taken into account by a cloud computing service provider are:

– Physical security
– Logical security
– Security and legal, political and technical certainty.

These types of security include as relevant aspects: confidentiality, authentication and availability, among others, all of them to guarantee the availability of work in the cloud. The concerns are the same as in the rest of the world with regard to security in cloud services, and have to do with the development of a project that resolves essential aspects such as who connects, who accesses, where access and under what conditions have certain access privileges. For this, it is necessary to review the conditions of the contract with the provider of cloud computing services, in order to ensure an adequate forecast of the issues related to the treatment and / or a transfer of personal data.

According to (Vizcaíno & Cruz Valencia, 2010) in the security magazine, the provider and the user should comply with the following guidelines to ensure the security and privacy of information in the use of the service:

Regarding the provider:

– Guarantee the user the security practices and procedures that are included in the service levels.
– Disclose to the user the geographic location of the information.
– Inform the user when the provider is obliged to deliver his information to a legal authority.
– Count in the terms of the service with a clause that guarantees that access to data is denied as a general policy.
– Apply the access requirements to the information imposed by the user.
– You may not claim ownership of any aggregate information, created, generated, modified, stored, or in any other way associated with the user's intellectual property, engineering effort or media creative.
– Specify what the provider can and can not do with the user's information.

ISSN: 2524-2113

– Provide at least one access mechanism.
– Ensure that the user's information is backed up and not mixed with other users' information.
– Guarantee that a robust encryption of information storage is used, which prevents access to it when it is recycled, disposed of or accessed by any means other than applications, processes or authorized entities.
– Destroying the information, when the user requests it, in all physical and logical locations.
– Deliver audit reports, which specify that your business continuity plans work.
– Explain how you monitor and control access to information made by your employees.

Regarding the user:

– Understand how privacy is maintained and make evident the commitment of this to the benefit of the client.
– Consider laws and directives of the country where the information is physically located.
– Carry out an evaluation of the information and systems proposed to be moved to the cloud.
– Conduct, if you have the necessary knowledge, an evaluation of the impact of privacy to identify and mitigate the risks derived from the privacy of information.
– Determine who should have access to the information, what their rights and privileges are, and under what conditions access is granted.
– Generate a default deny policy.
– Define and identify the classification of information.

In addition to the guidelines proposed by Vizcaíno & Cruz Valencia in the security magazine, in terms of the user we could add:

– Provide the authority with the information requested.
– Understand the sharing mechanisms where users are separated and the information they present.
– Encrypt the information stored in the cloud, as well as the one that is in transit.
– Accept from the provider the withdrawal mechanisms of information storage.
– Have plans for the conservation and destruction of information.

Business advantages and disadvantages offered by cloud computing

It is a reality that cloud computing has planted a novel scenario for companies, which have used this and technological advances to offer their goods or services trying to reach the largest possible market, so a list of the possible business advantages and disadvantages in the use of cloud computing.

Among the business advantages offered by cloud computing, we can list the following:

– Cost savings: they are only paid for the services that are used, since the additional costs are eliminated, for example the software licenses.
– Accessibility: provision in real time and shared information stored in the cloud from anywhere in the world, the only requirement being the connection to the internet.
– Speed: the information can be consulted at the moment you want, without having to wait for late downloads.
– Security: this is considered its main advantage, however it is not 100% safe, but more and more professionals are prepared to have the best security and reliability in the cloud, able to solve problems that arise.
– Multi-user structure: allows you to connect to different users, regardless of whether they are searching or using the same information.

Among the disadvantages that have been visualized for the activity of the company in its experience with cloud computig, we can mention:

– Privacy: this disadvantage is understandable, however cloud computing offers the opportunity for the user to determine with whom he shares or gives his information.
– Availability: if for any reason the service fails, you only have the possibility to wait for the provider to solve it.

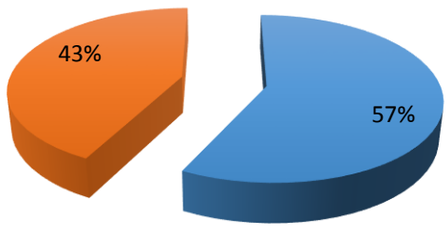
ISSN: 2524-2113

– Lack of control over resources: the user lacks access to services code.

Dependency: both the user and the provider must have a connection to the network to enjoy the cloud services.

Legal aspects of cloud computing in Mexico

The Digital Agenda of the National e-Mexico System, headed by the Ministry of Communications and Transportation, defines that it is a strategy of the national e-government to orient and promote the country's transition to the information and knowledge society, with the main objective accelerating the process of technological adoption in all areas of national life, intensifying and guiding its use to generate impacts on competitiveness, social and human development, as well as for the greater empowerment of citizens. Figure 1 shows the degree of availability of Information Technology (IT) in Mexican households, according to the National Institute of Statistics and Geography (INEGI), including fixed and mobile Internet users.



Graphic 1 Availability of IT (Mexico, 2015)
Source: INEGI(2016)

According to the Ministry of Communications and Transport (Mexico, 2015), the low international performance is explained by the persistence of the main inhibitors that characterize the digital divide in Mexico, of which:

People: There are 68 million Mexicans who are not Internet users, mainly in low-income and low-education sectors. The digital divide of people is inevitably transferredI to all institutional environments, notably companies and governments.

Connectivity: The high costs of connectivity and computing devices related to the income of individuals, companies and governments makes technological adoption difficult.

The contents: The low relevance of the contents in relation to people in conditions of vulnerability where the priorities are subsistence, makes the adoption of technology from its irrelevant perspective. (Mexico, 2015)

The author Valdés points out that the Digital Agenda has the following strategic objectives: Bridging the digital divide that separates Mexicans with access and without access to information and knowledge technologies.

Universalize broadband institutional and community connectivity, to achieve comprehensive coverage of schools, hospitals and health centers, government offices, and where government programs are provided to care for the population, as well as community access points, especially those that are required in marginalized areas. (Valdés T., Lex Cloud Computing, Legal Study of Cloud Computing in Mexico, 2013)

In this way, the Digital Agenda of the National e-Mexico System contributes to the use and development of cloud computing in Mexico, where there are aspects of the services that cloud computing offers having legal incidents, so its knowledge is relevant to avoid and avoid penalties of a legal nature. Within those aspects are:

– *Privacy*

One of the most important threats posed by cloud computing is the loss of the right to privacy, a human right guaranteed by various fundamental laws and international regulations. Currently, the right to protection of personal privacy charges and is very relevant, due to the manifest technological advances, which have increasingly caused the vulnerability of people's private lives. The right not to be disturbed in your privacy implies some aspects, but in the case of cloud computing, it has a direct impact on the control and handling of information and personal data collected in databases.

– *Security*

Ensure that suppliers have the necessary security measures, so that the information provided continues to have the characteristics of being reliable, secure and that a third party can not dispose of and make use of it.

ISSN: 2524-2113

– *Interoperability*

That users continue to have the possibility of choosing goods, services or technologies.

– *Permanence and Access to information*
The service provider must guarantee the access and content to the information until the moment in which the validity of the contract established with the users is fulfilled.

– *Availability*

The provider must provide users with sufficient services to ensure rapid response times and permanent access to stored information.

– *Clauses of rights of Suppliers and limitation of liability*

Users of cloud computing services should pay attention to those clauses where they mention the terms of access to cloud services, which can give providers rights over the information that is hosted on their servers.

– *Cloud Computing services to governments*

As the technology advances, the rules of contracting or guaranteed rights online are not advanced, which generates the government to come up with a value proposition of service in the cloud.

– *Taxes*

Several fiscal aspects must be taken into account by both providers and users. No matter which country it is or where it is, the fiscal aspects applicable to the jurisdiction of the State where the user is domiciled should always be considered.

All these aspects must be analyzed under the magnitude of the legislation that applies to cloud computing, since there are laws that require the confidentiality and security of information to be maintained, among which we can list the following:

– General Law of Professions
– Federal Labor Law
– Industrial Property Law
– Federal Law for Protection of the Consumer
– Federal Law of File
– Federal Law of Electronic Signature
– Commercial Code
– Federal Law on the Protection of Personal Data Held by Individuals

This legislation basically addresses the confidentiality and security of the information handled in the electronic media.

Regarding the **General Law of Professions**, whose purpose is to regulate the professional practice among the federal and local authorities, prescribing the way to prove the records, acts and procedures that within said function are carried out, as well as the warrant to preserve the secret professional in the exercise of the profession.

While article 134, section XIII of the **Federal Labor Law** mentions that it is the obligation of the worker to keep technical, commercial and product manufacturing secrets, in addition to reserved administrative matters, whose disclosure may cause harm to the company. Likewise, fraction IX of article 47 of the mentioned order prohibits the worker to reveal the secrets of factory or reserved matters to the detriment of the company, being the reason for the disclosure of the information, the termination of work without responsibility for the employer.

Following in the legal analysis, in the **Law of Industrial Property** addresses the issue of confidential information through the definition of what should be considered as an industrial secret in Article 82:

Considers an industrial secret to all information of industrial or commercial application kept by a physical or moral person in a confidential manner, which means obtaining or maintaining a competitive or economic advantage over third parties in the conduct of economic activities and in respect of which it has adopted the means or systems sufficient to preserve their confidentiality and restricted access to it.

With regard to sufficient means or systems in the preservation of the confidentiality of information, Article 83 of the same law makes reference that it must consist of documents, electronic or magnetic media, optical discs, microfilms, films or other similar instruments.

ISSN: 2524-2113

In addition to this, it is contemplated that any person who, because of his work, employment, position, position, performance of his profession or business relationship, has access to an industrial secret of which he has been warned about his confidentiality, should abstain to disclose it without just cause and without the consent of the person who keeps said secret, or of its authorized user[1]. If you are a natural or legal person and hire a worker who is working or has worked, or a professional, consultant or consultant who provides or has provided their services for another person, in order to obtain industrial secrets from it, the number 86 of the Industrial Property Law establishes that he will be responsible for the payment of damages and losses caused to said natural or legal person.

This same Law of Industrial Property considers a crime by complaint the disclosure of an industrial secret, the sanction being a prison sentence of 2 to 6 years in prison and a fine of one hundred to ten thousand days of the general minimum wage in force in the Federal District[2].

As for the **Federal Law of Consumer Protection**, a chapter is provided regarding the rights of consumers in transactions made through the use of electronic, optical or any other technology. Being the article 76 BIS the one that lists the legal dispositions related to it, highlighting some that must be fulfilled:

1. That the provider will use the information provided by the consumer in a confidential manner, unable to disseminate it or transmit it to other suppliers outside the transaction, unless expressly authorized by the consumer or competent authority.
2. That the supplier must use any of the available technical elements to provide security and confidentiality to the information provided by the consumer and inform the consumer of the characteristics of said elements.
3. The consumer has the right to know all the information about the terms, conditions, costs, additional charges, if any, forms of payment for the goods and services offered by the supplier.

The **Federal Law of Archives** establishes the provisions that allow the preservation of the archives in possession of the Powers of the Union, as well as the protection, dissemination and access of private archives of historical, technical, social, cultural or scientific importance.

With regard to the **Commercial Code**, its Second Title dedicated to Electronic Commerce, it is divided into four chapters, the first of which refers to data messages, a subject in which cloud computing is included. From this we can mention that Article 89 of this Code indicates that:

The activities regulated by this Title will be subject in their interpretation and application to the principles of technological neutrality, autonomy of will, international compatibility and functional equivalence of the Data Message in relation to the information documented in non-electronic media and the Electronic Signature in relationship with the signature autograph.

In this article 89 some definitions referring to electronic commerce are mentioned, giving indications that cloud computing begins to be regulated, these are: recipient, digitization, issuer, electronic signature, data message, certification service provider and systems of information, which permeate to act legally under the premise of cloud computing services (for more information see the law and the article mentioned).

The mentioned definitions are transcribed from this article 89, in order to know that cloud computing:

– Recipient: The person designated by the Issuer to receive the Data Message.

– Digitization: Migration of printed documents to data message, in accordance with the provisions of the official Mexican standard on digitization and preservation of data messages issued by the Ministry of Economy for that purpose.

[1] Article 85 of the Industrial Property Law.

[2] Article 224 of the Industrial Property Law.

ISSN: 2524-2113

– Electronic Signature: The data in electronic form consigned in a Data Message, or attached or logically associated to it by any technology, which are used to identify the Signatory in relation to the Data Message and indicate that the Signatory approves the information contained in the Message of Data, and that produces the same legal effects as the signature autograph, being admissible as evidence in court.

– Data Message: The information generated, sent, received or filed by electronic, optical or any other technology.

– Certification Services Provider: The person or public institution that provides services related to electronic signatures, issues certificates or provides related services such as the preservation of data messages, the digital time stamp and the digitalization of printed documents, in the terms that be established in the official Mexican standard on digitization and preservation of data messages issued for that purpose by the Ministry of Economy.

– Information System: Any system used to generate, send, receive, file or otherwise process data messages will be understood.

As we can see, cloud computing uses the concepts presented in order to act legally under the premise of cloud computing services.

The **Federal Law of Electronic Signature** establishes the regulation of the advanced electronic signature, the electronic certificate and the related services of its surroundings (Téllez, 2013), in addition it intends to homologate the advanced electronic signature with the advanced electronic signatures regulated in other legal ordinances.

Among the concepts to be highlighted in this law, which go hand in hand with cloud computing and the services it offers, are:

a) Electronic Media: are the technological devices for the processing, printing, deployment, conservation and, where appropriate, modification of information.
b) Message of Data: is the information generated, sent, received, filed or communicated through electronic communication means, which may contain electronic documents.
c) Website: is the website that contains information, applications and, where appropriate, links to other pages.

However, despite the fact that this law represents an advance talking about electronic information systems, it is an order that aims to regulate the performance of public entities and dependencies, their servers and individuals that use the advanced electronic signature in terms of of this Law.

Although this does not mean that the same public entities do not use the services of cloud computing. In fact, we start from the reality that is shown to us today, since many of the services that are offered by public agencies are through the web, materializing a part of what we call e-government or electronic government.

The e-government and cloud computing are currently an indissoluble binomial, the first tended an electronic network for various services or public activities, understood as the use that the public function made of ICTs in order to provide the population with better and faster services by their agencies, through the organization and automation of their processes, especially in the procedures they offer, optimizing the resources of each public entity from financial to human, while cloud computing presents the e-government with the ability to manage and store large amounts of information streamlining your work. All of the above, taking as frame of reference a, perhaps, incipient legislation.

To conclude the legal analysis, we have the **Federal Law for the Protection of Personal Data Held by Private Parties** (FLPPDHPP) that entered into force on July 5, 2010, being its first article that establishes its legal-public scope, having as its object the protection of personal data in the possession of individuals, in order to regulate their legitimate, controlled and informed treatment, in order to guarantee privacy and the right to self-determination of people.

ISSN: 2524-2113

Besides, its purpose is to establish and maintain administrative, technical and physical security measures that allow protecting the personal data of any individual against damage, loss, alteration, destruction or unauthorized use, access or treatment, placing people in the center of state guardianship.

The day after the issuance of this law, the companies of all the activities were forced to publish privacy notices and protect the personal information that they could find in their databases, such as financial, banking and financial institutions. credit, insurers, media, telephone companies, commercial, industrial, service, hospitals, airlines, schools, doctors, laboratories, law firms, accounting firms, advertising companies, department stores, restaurants, car agencies, etc.

And it is that this law is addressed to private individuals or individuals of a private nature, who carry out the processing of personal data, in accordance with its Article 2.

It has been mentioned that the Mexican Data Protection Act contains clear and respectful rules regarding the privacy of information provided by individuals, as a result of international principles accepted and regulated in other sovereign States and various international organizations.

Taking this as a reference, we highlight some key concepts listed in the FLPPDHPP, based on accepted international principles, which frame cloud computing, as they are

1. Privacy Notice: Physical, electronic document or any other format generated by the person in charge who is put at the owner's disposal, prior to the processing of their personal data.

From the privacy notice, it should be noted that companies that make use of cloud computing, must manifest it clearly on their electronic pages, where the user can read and accept the conditions provided by law.

2. Databases: The ordered set of personal data referring to an identified or identifiable person.

3. Blocking: The identification and preservation of personal data once the purpose for which they were collected has been achieved, with the sole purpose of determining possible responsibilities in relation to their treatment, up to the legal or contractual limitation period of these. During this period, personal data can not be processed and once this has elapsed, it will be canceled in the corresponding database.

4. Consent: Manifestation of the will of the owner of the data through which the treatment of the same is effected.

Again, for companies whose object is borrowed through cloud computing, the manifestation of the will will be ticking a box accepting the conditions described by the company.

5. Personal data: Any information concerning an identified or identifiable natural person.

6. Sensitive personal data: Those personal data that affect the most intimate sphere of its owner, or whose misuse could give rise to discrimination or entail a serious risk to it. In particular, those who can reveal aspects such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions, sexual preference are considered sensitive.

7. Source of public access: Those databases whose consultation can be carried out by any person, with no more requirement than, in his case, the payment of a consideration.

It is established in the legislation that if the personal data are violated by the companies that store them, that is, if they are lost, if there is unauthorized access or if they are hacked, the holders of the data should be informed as soon as possible personal information, so that they can take the necessary and necessary measures in defense of their rights. (Gomez, 2012)

The Federal Institute of Access to Information (IFAI), has stated that the most important thing to know about the FLPPDHPP:

ISSN: 2524-2113

- A personal fact is any information related to the individual.
- They are personal data: the name, address, telephone, photograph or fingerprints, as well as any other data that serves to identify the person.
- The person owns their own personal data and only she decides how, when, to whom and for what she gives her personal information, except for the exceptions established by law.
- It is important that the person takes care of their personal data for security reasons, besides being their right.
- The data or personal information must be protected against misuse such as: identity theft, illegal transmissions or unauthorized access.
- The Law regulates the conditions in which companies must use personal data.
- There are sensitive data requiring greater protection, they are considered as such: racial or ethnic origin, health status, genetic information, religious, philosophical and moral beliefs, union affiliation, political opinions and sexual preferences.

To these concepts are added the legal principles that must be met by companies, individuals or corporations in the processing or storage of information or personal data in physical or electronic form, which are: consent, lawfulness, purpose, information, quality, loyalty, responsibility and proportionality.

Starting from the fact and right that, in the treatment and handling of personal data, it is assumed that there is a privacy agreement, understanding this as the trust that is deposited between two or more people, with respect to the personal data or information provided, will be treated as agreed by the parties, being subject to the consent of the owner[3]. Said consent may be expressed expressly or tacitly, for the first case may be verbal, in writing, by electronic means, optical or by any other technology, or by unambiguous signs.

While tacitly it will be when the processing of your data or information, when you do not state your opposition and you have made yourself available to the privacy notice.

This leads us to reference the content of the privacy notices that must be met by those responsible for the handling of information, including those that are dedicated to cloud computing services, namely:

1. The identity and address of the person responsible for collecting them.
2. The purposes of data processing.
3. The options and means that the responsible party offers to the holders to limit the use or disclosure of the data.
4. The means to exercise the rights of access, rectification, cancellation or opposition.
5. In your case, the data transfers that are made.
6. The procedure and means by which the responsible will communicate the holders of changes to the privacy notice. (Article 16 FLPPDHPP)

Following the privacy notice and as indicated by the FLPPDHPP, it must be made available to users through printed, visual, digital, sound or any other technology. In the event that they are obtained directly from the owner by any electronic, optical, sound, visual, or through any other technology, the responsible must provide the owner immediately, at least information regarding the identity and address of the person responsible that collects them, as well as the purposes of data processing; as well as providing mechanisms for the owner to know the full text of the privacy notice. Currently have established cloud computing agreements, which provide for public or private agencies allow the outsourcing of services, while providers offer security, privacy and protection of personal data. If the provider complies with the privacy policies and complies with the regulations that subscribe to the legislation, it could be affirmed that the provider is really reliable and legally established.

Undoubtedly, cloud computing or cloud computing has been a necessary tool for the storage and handling of information, giving a special and confidential treatment of the data that customers or users make of various services that companies offer on the web, the responsibility of these part of the confidentiality notice and later with the handling of the information found in the web servers.

[3] Article 7 FLPPDHPP

ISSN: 2524-2113

Case study: Legal applications in cloud computing

In this section it is assumed that privacy policies and conditions of use are a common denominator in commercial and public websites. In Cloud Computing all pages and / or web services have this section of Privacy Policies and Conditions of Use. The following cases are explored:

– Dropbox

Dropbox is a cloud server that allows you to store, host and share files through a personal account, either for free or for a fee. Therefore, in its Privacy Policies we can find that they apply the Data Protection Law. Dropbox specifies the information that they require to be their clients, likewise establishes the way in which the information provided will be used and under what security regime and Privacy.

Dropbox service conditions in which it explains what happens with the files they share and the permissions that they have, making the person responsible for the information they share in the files, briefly detailing the uses accepted by creating an account, reiterating that in The moment the client no longer wants the service, a cancellation (Opt-out) is made without any problem.

– Storage of email account (Hotmail, Gmail the most common)

Google (Gmail)

Drive is the storage option offered by Gmail, by having an account with this email provider, it offers us a space to store files that we can have available through our account, anywhere, anytime, as long as we count with Internet connection. Google in the privacy policies, tells us the conditions of service (Google, s.f.), which says:

[...] you will remain the owner of the intellectual property rights you have over that content. In short, what belongs to you, yours is.

We do not claim ownership of any of your content, which includes the texts, data, information and files you upload, share or store in your Drive account.

Our Terms of Service allow us to provide the services you are looking for. So, if you decide to share a document with someone or want to open it on another device, we can offer you that functionality.

You control who can access your files saved in Drive. We will not share your files and data with anyone except to the extent specified in our Privacy Policy.

– We will not publish any private documents.
– We will not use any private documents for marketing or promotional campaigns.
– We will save your data as long as you want.
– You can take the data with you if you decide to stop using Google Drive.

Microsoft (Hotmail, Live, Outlook)

OneDrive - from Microsoft - like Gmail, offers storage by having an account with this email provider (Outlook, Live, Hotmail), in this one space we can store files, which we can have available through our e- mail, anywhere, anytime, provided you have an Internet connection.

In the Microsoft privacy statement (2017), it details us about:

– Personal information that they collect
– How they use personal data
– Reasons for sharing personal data
– How they access and control personal data
– Cookies and similar technologies
– Microsoft account

It is important to note that storage options are not the only thing that these email providers offer, there is also the office software (applications for text editing, spreadsheets, digital presentations among others), collaborative work (calendars, virtual communities), among others.

Conclusions

As we already examined, cloud computing or cloud computing has its main foundation in the remote management of information.

ISSN: 2524-2113

Companies, public entities and organizations transfer large amounts of information to servers belonging to third parties (other companies dedicated to this). This brings with it several implications or legal consequences, even more in the case when the data is hosted or stored in servers in other countries, converging two or more jurisdictions, arising the need to determine legal and contractual aspects applicable to the case. In several countries laws have been enacted where their main objective is to protect information, being Sweden in 1973 the first country in the world to have a data protection law, following the example of the United States in 1974 and others in Europe western.

On the other hand, Mexico has enacted its own data protection law, which is one of the newest in the world; However, in the analysis of this law and other correlatives of the subject, it can be identified that they do not explicitly contemplate the processing of personal data in cloud computing services, while in countries of the European Union, Argentina, Canada and others, consider safe ports to countries that have the possibility of transferring stored data in a secure manner and protected by the contract and data protection law of their country.

Now, starting from the environment of the information society, Mexico has a significant advance in the digital economy and electronic government, as already explained in the development of this research; however, some tasks are still missing. The current mandate of the government is crucial in the information age, since the combination of technological advances with new forms of operation and the handling of information stored in the cloud, will make it more efficient and effective. Our country has important efforts in this area (trinomial: ICTs-operation processes-handling and storage of information in the cloud); However, there is still no comprehensive and legal public policy on the matter, which concentrates efforts and brings together the agents involved in the development, competitiveness and technological innovation worldwide.

As a diagnosis, we could say that our country needs to create strategies to promote small and medium-sized companies that are obsolete with regard to technology, as well as developing media outlets that report the benefits, advantages and disadvantages of cloud services.

The State for the web services it offers must have the objective of optimizing public spending by having a better treatment of the information it has and generates inside and outside of its dependencies, in order to increase the quality and speed of its services with the population, being the cloud computing the key piece to start and start up as part of the public services of the country.

Regarding the private area, users of the services or products offered on the web, seek not only the versatility of the search for information, but also the security and privacy of the data or information they share in an application, or in a purchase, etc.

The user's peace of mind is based on the fact that their information has been delivered in order not to be violated, that the storage and management of the information is professional, that sufficient means have been adopted for the storage of their information, with cloud computing being a means to achieve those objectives.

Undoubtedly and after analyzing the relevant legislation, there are important legal challenges for the success in the adoption and development of cloud computing from the public as well as the private perspective, with the two priority issues to be addressed: privacy and security of information on the web. Explain clearly the results obtained and the possibilities for improvement.

References

Gomez, J. (2012). Seguridad de la Información. Recuperado el 1 de Julio de 2016, de Seguridad de la Información: http://www.joelgomez.mx/blog/?tag=seguridad-de-la-informacion

Google (s.f.). Condiciones de Servicio de Google Drive. Recuperado el 1 de Julio de 2016, de Ayuda de Google Drive: https://support.google.com/drive/answer/2450387?hl=es#

IBM (2017). IaaS PaaS SaaS - Modelos de servicio cloud. Recuperado el 15 de Diciembre de 2017, de IBM Cloud: https://www.ibm.com/cloud-computing/es-es/learn-more/iaas-paas-saas/

ISSN: 2524-2113

INEGI (2016). Encuesta nacional sobre disponibilidad y uso de tecnologías de la información en los hogares, 2015. Recuperado el 15 de Diciembre de 2017, de: http://www.inegi.org.mx/saladeprensa/boletines/2016/especiales/especiales2016_03_01.pdf

Microsoft (2017). Declaración de privacidad de Microsoft. Recuperado el 22 de enero de 2018, de: https://privacy.microsoft.com/es-mx/privacystatement

Systems, A. (2015). Copias de seguridad. Recuperado el 1 de octubre de 2016, de Copias de seguridad: http://www.accurate-systems.es/Backup_Seguridad.html

Téllez, J. V. (2013). Lex Cloud Computing. Estudio Jurídico del cómputo en la nube de México. México: DR.

Unión, C. d. (8 de Junio de 2009). Código de comercio. Recuperado el 1 de Septiembre de 2016, de Código de comercio: http://www.oas.org/juridico/spanish/mesicic3_mex_anexo8.pdf

Legisgrafía:

– General Law of Professions
– Federal Labor Law
– Industrial Property Law
– Federal Law for Protection of the Consumer
– Federal Law of File
– Federal Law of Electronic Signature
– Commercial Code
– Federal Law on the Protection of Personal Data Held by Individuals

ISSN: 2524-2113