Abstract— Even though the services provided and the adoption of cloud computing have started revolutionizing the business domain, the concept still remains an uncharted area with respect to many dimensions. Cloud computing, in the most general sense, refers to an application, a service, a resource or a platform that can be used via the Internet where users subscribe to a set of service definitions rather than the details of the service implementation. The novelties of the services and business processes provided by cloud computing together with the expected growth of cloud services, make it important to address the legal and economic aspects, as these two affect and are being affected greatly by cloud computing and its use by individuals and businesses. The three major usage models (service levels) of cloud computing, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), are inherently interrelated with each other but each has specific characteristics that make it a requirement to address legal and economic issues separately. Cost and expense items from different sources, including technological, operational and management expenses, result to a complex cost model, making it difficult to decide on what is the reasonable price of the offered service. On the other hand legal implications represent and address constraints imposed to the offered services, sensitive data and intellectual properties, contracts, service quality, legal risks of adaptation, and uncertain jurisdiction for Internet activities in geographically distributed cloud data centers. The existing literature points out that legal and economic aspects are closely interrelated to each other as economic factors may result to more cost-effective cloud computing models, while legal factors will always constrain and weaken any potential cost benefits. The aim of this paper is to briefly introduce the legal contractual, economic and pricing issues related to overall cloud computing and also specific to service levels as they are covered in the cloud computing literature, and to provide a starting point for the discussion on how these can be addressed within the Turkish Law.

Keywords— Cloud computing, cloud computing usage models, cloud computing pricing, cloud computing legal issues

I. INTRODUCTION

Cloud computing (or cloud services) is a new and disruptive paradigm of information technologies (IT) delivery and deployment. This new paradigm by providing highly appealing features such as rapid deployment, high scalability and flexible pricing, has revolutionized the IT and the business domain, and thus has become one of the most talked buzzwords of the last few years, often regarded as a one “all-embracing concept” and as a single technology by many people [1, 2, 3]. However, cloud computing is not one single technology, nor is it one single architecture [4] but a computing and business phenomenon that comprises a number of aspects. The most widely accepted definition of cloud computing and services is given by the NIST1 as [5]:

“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”.

At the same definition, five essential characteristics are identified in cloud computing model, namely i) on-demand self-service, ii) broad network access, iii) resource pooling, iv) rapid elasticity and v) measured service [5]. The three major cloud usage (service) models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The three models and the components that are provided to the user to manage them are given in Figure 1 [6].

A. Infrastructure as a Service (IaaS)

IaaS providers offer computers (physical and virtual machines) and other resources as raw computing, memory, storage, and network transfer capabilities for custom solutions. The customer is given the capability to provision processing, storage, networks, and other fundamental computing resources, and where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components [5].

B. Platform as a Service (PaaS)

PaaS providers offer the necessary computing platform and development environment for deploying new applications onto the cloud. These may include programming language execution

---

1 National Institute of Standards and Technology
environments, databases and web servers. The customer is given the capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment [5].

C. Software as a Service (SaaS)

SaaS is the model that most individual customers are familiar with. SaaS providers offer the use of the applications (application software) and databases running on the provider’s cloud infrastructure. The customer is given the capability to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings [5].

![Figure 1 Cloud Service Models](image)

The rest of the document is organized as follows: In Section 2 the legal and economic issues of cloud computing that are applicable to all service models are briefly discussed. Section 3 introduces the contract related issues, specific to service models. Section 4 concludes the paper.

II. LEGAL AND ECONOMIC ISSUES RELATED TO ALL SERVICE MODELS

A. Cloud Service Contracts

A cloud service contract, or as referred to in [2] the Terms of Service (ToS), is an agreement between the cloud service provider and the customer, including terms and conditions, service level agreements, acceptable user policies, and privacy policies. The cloud service provided by the service provider may be a paid or a free one; this study focuses only on paid services. In such cloud service contracts the content, scope and quality of cloud services to be provided need to be clearly defined [7].

A Communication by the European Commission [8] clearly differentiates between the traditional contracts in IT outsourcing and cloud service contracts. In traditional IT contracts arrangements were typically negotiated and related to data storage, processing facilities and services defined and described in detail and up-front. However, cloud service contracts essentially create a framework in which the users have access to infinitely scalable and flexible IT capabilities according to their needs. Nevertheless, the Report [8] states that currently the greater flexibility of cloud computing is often counterbalanced by reduced certainty for the customer due to insufficiently specific and balanced contracts with cloud providers. Furthermore, many cloud service contracts limit the liability of the service provider to a level that is not in line with the potential risk of the service, and even though that risk is much higher compared to traditional IT outsourcing still the cloud service contracts resemble typical software licenses [9].

Cloud service contracts appear in a wide variety of forms, ranging from simple standardized “click wrap” contracts offered under non-negotiable bulk business standard conditions, to multilayered sets of terms and conditions and individually negotiated contracts [10, 7, 11]. Service providers often use complex contracts or service level agreements with extensive disclaimers as non-negotiable contracts because of the complexity and uncertainty of the legal framework for cloud services [8]. The European Commission names these standard contracts as “take-it-or-leave-it” contracts, and states that even though they might be cost-saving for the provider, they are often undesirable for the customers and may also impose the choice of applicable law or inhibit data recovery [8]. Individual users and small to medium sized business due to their limited scale, size and resources may not have the leveraging power to enter into negotiations with service providers. However, negotiations are customary for cloud computing contracts above a certain contract volume, or if the customer appears to be of significance to the supplier as a reference [7], but even then larger companies have little negotiation power and contracts often do not provide for liability for data integrity, confidentiality or service continuity [8]. In case that the negotiations on contract terms are possible, such customers may prefer individually negotiated contracts for liability protection because the parties can tailor the terms and conditions appropriate to the level and degree of contractual obligations and performance [10]. Examples of non-negotiable contract statements are given by [9] as:

> “We and our licensors shall not be responsible for any service interruptions, including, without limitation, power outages, system failures or other interruptions, including those that affect the receipt,

2 The overall relationship between the customer and the provider, including the commercial terms, whether the service is paid for, legal clauses such as choice of law, and disclaimers [2].

3 Associated only with paid-for services, they define the level of service the provider aims to deliver together with the process for compensating customers if the actual service falls short of that [2].

4 The permitted (or in practice, forbidden) uses of the service [2]

5 The provider’s approach to using and protecting the customer’s personal information and/or data [2].
Another example from the non-negotiable terms and conditions is the below excerpt from the “Terms and Conditions for Microsoft Office 365” [12]:

“3.5. It is hereby expressly agreed and acknowledged by O2 and the End User that:

3.5.1. O2 and Microsoft make no representations or warranties whatsoever, express or implied, including without limitation, any representation or warranty with respect to the design, compliance with specifications, quality, operation, the merchantability or fitness of the online services for a particular purpose, or issues regarding IPR infringement, title and the like;

3.5.2. the End User hereby waives to the maximum extent permitted by law any rights and remedies conferred upon the End User under any relevant legislation, including but not limited to the Sale of Goods and Supply of Services Act, 1980 as amended, and those rights now or hereafter conferred by statute or otherwise;

3.5.3. O2 shall not be deemed to have made, be bound by or liable for, any representation, warranty or promise made by Microsoft in respect of the Online Services;

3.5.4. O2 shall not be liable for any failure of the Online Services or any delay in the availability thereof; and

3.5.5. the Customer has selected the Online Services without O2’s assistance.”

Such terms and conditions in the contract prepared by the service provider pose an important problem with respect to limiting and even removing the customers’ rights.

In [7], the authors describe the various legal requirements relating to cloud service contracts that must be observed under Swiss law. The service descriptions and service level guarantees, especially with regard to scalability, availability, performance, data security etc., should be reviewed, and if necessary, negotiated and amended to ensure they meet customer requirements. The regulations on duration of contract, termination and exit management are important for avoiding a vendor lock-in. Standard supplier contracts often provide for short periods of notice and the customer must check whether these are sufficient for it to obtain a new solution for cancelled cloud services, whether a longer period of notice needs to be negotiated. If the support of the supplier is necessary for the retransfer of data and applications, the corresponding support services and their cost have to be specified as precisely as possible in the contract. Suppliers’ contracts often contain extensive disclaimers. If the disclaimer proves to be non-negotiable, the customer must decide, having given due consideration to the benefits associated with the cloud offer, the probability of an incident and the associated potential for damage, whether the contract is ultimately acceptable.

However, many cloud service contracts are “click wrap”, meaning that the contract between the service provider and the customer is concluded by just clicking the “Accept” button in an electronic form. At this point, two important questions arise with respect to the new Turkish legislation:

- Contract texts, that are prepared by the service provider in advance and in reality there is no possibility for the customer to read and understand them during the clicking process, are they part of the framework contract?
- If the answer to the previous question is “yes”, do the terms and conditions written in these contract texts that have not been negotiated, bind the users?

With the new Turkish legislation [13, 14] special legal control rules have been introduced with respect to standard terms and conditions in the contracts. Unlawful terms and conditions are accepted to be “unwritten” (TBK articles 21,115) [15].

The European Commission in its Communication to European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions dated 27.9.2012 [8] identifies that the cloud service contract problems are related to concerns over data access and portability, change control and ownership of the data. The report clearly pinpoints several contract based concern examples such as:

> “how liability for service failures such as downtime or loss of data will be compensated, user rights in relation to system upgrades decided unilaterally by the provider, ownership of data created in cloud applications or how disputes will be resolved”.

Moreover, customers are often unaware of their relevant rights especially including the applicable law and commercial matters related to contract law questions. Although existing EU legislation protects users of cloud services, the European Commission’s Communication [8] proposes several steps to overcome the existing contract based problems:

- Development of model contract terms,
- The use of self-regulatory agreements or standardization,
- The development of European model contract terms and conditions based on an optional contract law instrument in order to create transparent and fair cloud services contracts, especially for contracts with customers and small sized companies.

B. Protection of Personal Data

One of the main legal considerations is the protection of the data stored in the cloud as part of the cloud service contract. The stored data should not only be protected by terms of the contract concluded between the service provider and the customer, but also with legal regulations, especially with regulations focusing on the protection of personal data [16]. However, when the data storage locations and the national security concerns are taken into account it is not possible to state that an absolute data protection can be accomplished. At this point, the responsibility of the service providers becomes the issue. Moreover, the mandate of the service provider to specify some other service provider as a subcontractor and the extent of this mandate are also very important with respect to data protection.

As the European Union (EU) still has the greatest number of jurisdictions with data protection statutes [2], we address the subject of data protection through the EU legal perspective. The EU Data Protection Directive (DPD) adopted in 1995 [17] applies to personal data, which is defined in the same directive as:
“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”

The DPD aims to protect the rights and freedoms of persons and sets strict limits on the collection and use of personal data with respect to the quality of data, the legitimacy of data processing, the information to be given to the subject and the right to object to the data collection [18]. However, stricter regulation applies to the processing of “sensitive data”, that is personal data revealing ‘racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership’, ‘data concerning health or sex life’, and criminal offences or convictions [2]. Moreover, data that is not, or ceases to be, “personal data” may be processed, in the cloud, or otherwise, free of data protection law requirements [2].

To identify the key obligations and liabilities of cloud service providers with respect protection of personal data, it is important to understand whether the service provider is a “controller” or a “processor”, complex terms introduced by the EU DPD. The controller is defined as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data” and the processor as “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller” [17]. Depending on the types and characteristics of the provided services a cloud provider can be regarded as a controller, a processor, both or neither [2].

The Safe Harbor framework [19], developed to ensure the safe passage of data from Europe to the USA, requires that the companies that want to be a part of the agreement have to comply with a number of rules, including [18]:

- The notification of individuals about the purposes of data collection
- The access for individuals to personal information about them
- The obligation of the company to protect personal information from loss, misuse and unauthorized access

However, the regulations of the DPD and Safe Harbor framework are not enough to guarantee the protection of transnational data from Europe to USA as the USA Patriot Act, signed into law in 2001, affects not only data that is stored in the USA in accordance with the Safe Harbor Agreement but also data that is physically stored in Europe [18, 20]. A striking example of this is given in [18]:

The latter case is also relevant when the data is being stored by a European company that is a subsidiary of an American company. Confirmation of this point came directly from Microsoft. A company representative was asked at the launch of their new cloud service Office365 whether Microsoft can

“... guarantee that EU-stored-data, held in EU based data centers, will not leave the European Economic Area under any circumstances — even under a request from the Patriot Act.”

The reply was:

“Microsoft cannot provide these guarantees. Neither can any other company.”

The aforementioned subject has been voiced clearly in the German Parliament with a parliamentary question with date 31.01.2013, consisting of questions as long as seven pages, thus pointing out the extent of the problem [21].

As of January 2012, the European Commission has announced a draft European General Data Protection Regulation [22] to replace the DPD from 1995, aiming to build a modern, strong, consistent and comprehensive data protection framework for the EU and to reinforce the individuals’ fundamental rights to data protection. The new regulation introduces an explicit obligation for data controllers to delete an individual’s personal data if that person explicitly requests deletion and where there is no other legitimate reason to retain it.

In Turkey, the government bill related with the general regulation of protecting personal data (Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı) has not become a law for many years, and finally it has been proposed once again to the Parliament on 26/12/2014. The “Code on the Regulation of Electronic Commerce” no. 6563, has been accepted on 23/10/2014 and has been put onto effect on 1/5/2015. The Article 10 titled “About protection of personal data” of this Code states [23]:

“The service provider and the intermediary service provider:

a) are responsible of the storage and security of the personal data that they procured with transactions conducted within the frame of this Code

b) cannot transfer to third parties and cannot use for other purposes the personal data without the explicit permission of this person.”

C. Which Laws Apply to Cloud Computing

In Turkey, the applicable law for Private Law transactions that do have the element of foreignness is regulated with the “International Private and Civil Procedure Law” no. 5718. According to the article 24 of the aforementioned law, contractual claims are subject to the Law explicitly selected by the contracting parties. This selection can be realized by the contracting parties at any time, as long as this is not contrary to the public order.

In cloud service contracts the storage location of the data has a distinctive structure. More than one locations can appear as elements of foreignness, as people situated in different geographical locations will require to access their data. For example, the Office 365 cloud application states to its Middle Eastern customers that their data centers are primarily located in Holland and Ireland, whereas the backup data centers are mostly located in the USA. In a concrete case it has been revealed that the damaged data was scattered as follows: 20% in France, 30% in Argentina and 50% in Greece [16]. As it is observed, the move of data clouds in a transnational fashion, results to issues of conflict of laws. Therefore, it is important to agree upon the applicable law through the contract between the service provider and the customer.

In the event that the data stored in the cloud is damaged or lost by actions of third parties other than the service provider, then this is a case of a tort. According to the Article 34 of the International Private and Civil Procedure Law, tort damages are
subject to the law of the country where the tort has taken place. In the event that the tort and the tort damage have occurred in different countries, then the law of the country where the tort damage has incurred, is applied. Moreover, in the aforementioned law, an exceptional rule (escape clause) exists: in the case that the tort damage is more closely related with another country, then the law of this country is applicable [24, 16, 25]. On the other hand, the party responsible from the tort and the aggrieved party do have the option to select the applicable law, following the realization of the tort.

D. Overall Economics of Cloud Computing

The adoption of cloud services by customers in most cases is based on economic factors. As argued by Armbrust et al. [26], the economic appeal of cloud computing is not only on the fact that it converts capital expenses to operating expenses but mostly because it allows the use of the “pay as you go” (pay-per-use) model; a term that directly captures the economic benefits of the cloud customers. In the “pay as you go” model the customers pay for the use of computing resources on a short-term basis when these services are required and they let them go when these are no longer necessary. Even though in some service models this can be more expensive than purchasing the actual computers, the cost is outweighed when elasticity and risk transfer are considered [26]. Kansal et al. [27] state that the pricing schemes of the service providers may vary based on different provisioning of services and types of customers and classify broadly the pricing models in cloud computing on the basis of usage as subscription based, pay-per-use and hybrid pricing. In the subscription base pricing, advanced reservation of resources required for a specific time period is allowed by signing a Service Level Agreement. In the pay-per-use model the resources are provided on-demand, on the fly and the consumed resources are charged per unit of time on usage basis. Finally, the hybrid pricing model is an intermediate one between pay-per-use and subscription, where dedicated servers must be provided in advance for a period of time but additional resources can be requested on demand basis and billed at per-use basis [27].

Organizational adoption of cloud computing services in general is not an easy and inexpensive process, as it may require significant transformation of the existing IT systems and services of the organization [3]. Therefore, a thorough investigation of the cloud migration costs and expected values must be conducted to justify such a change, independent of the cloud service model planned to be acquired.

Williams [4] proposes a framework consisting of several metrics for measuring the financial value of critical components in the existing IT system and the planned cloud computing platform. These metrics should be methodically analyzed by any customer planning to procure cloud services, in order to justify the costs. The direct or financial metrics that can be used to measure business performance, such as net present value, return on investment etc., can be used to also in the assessment of a cloud service. However, special focus is given here to the indirect metrics as described and put forward by Williams [4]. The Total Cost of Ownership, widely used by cloud service providers to demonstrate the offsets associated with migrating to cloud, is defined as the sum total of all associated costs related to the purchase, ownership, usage and maintenance of an IT [4]. Martens et al. [28] give an overview of the different identified cost types associated with cloud computing, namely strategic decision, selection of cloud computing services and cloud types, evaluation and selection of service provider, service charge, implementation, configuration, integration and migration, support, initial and permanent training, maintenance and modification, system failures and backourcing or discarding. Availability, one of the most widely used performance measurements, is the amount of time a service is accessible or usable in an overall specific time window [4]. Cloud systems may not be available because of conservation, power outages or denial of service attacks; therefore, it is important to assess the availability of a cloud service also with the length of time between failures and the length of time needed to resume operation after failures [29]. Time to Market measures the time to implement a new application or to go to market with a new service, and it is a critical measure of a company’s capability to execute as it shows the IT department’s ability to support businesses while remaining flexible and agile [4]. Increased time to market denotes that the company is in a disadvantaged position compared to its competitors, such increases may be the result of broken processes, waste and inefficiencies in the IT supply chain [4]. Churn Rate, a critical measure of the overall performance and closely related to time to market and availability, shows the number of customers an organization has lost within a given time period [4].

III. CONTRACT ISSUES SPECIFIC TO SERVICE MODELS

In cloud computing contracts there is a wide spectrum of services provided, which services can be arranged in different flexible combinations. This makes it difficult to classify this combination of services as a single contract. However, the classification of the contract is of significance to the contracting parties. In legal regulations standard contract types are already defined individually, and these legal regulations contain specific guarantee obligations. Moreover, cloud service providers mostly prefer to conclude standard contracts with their customers. However, these standard contracts are subject to content control and in the case that the guarantee obligation of the service providers towards the customers is reduced significantly then the contract clause would be deemed invalid. Therefore, it is important to identify predominant contract types for each cloud computing service model, based on the specificities of the service model in question.

Cloud services are based on the handing over of computing resources and services for a specific period of time to the customer, for the exchange of some fee. However, the obligations of the service provider may include additional services. In this case, characteristics of further contract types may come into question, e.g. contract of work, contract of mandate, labor contract [30, 31, 32]. Cloud services contracts, in principle are composite contracts where the predominant element is the rental law [33, 34]. In the contents of these contracts, the guarantee that the service will be available is of great importance. In this regard, a sample verdict is this of the German Supreme Court that has deemed invalid the contract clause that stated that the maintenance periods of the servers will be not included in the calculation of the time periods that the service was available (availability) [35].
The legal aspects of cloud computing with respect to licenses come into prominence when the application software streams from the service provider (cloud) to the customer (local personal computer). However, this is an exceptional case and is not covered in this paper.

Determining and agreeing upon the exit options that will be followed at the termination of the service are “sine qua non” of every cloud contract.

In the SaaS model, the fact that the procured service may result to the customer becoming dependent to the service provider and their services, must be taken into account. Moreover, following the expiry of the SaaS contract, not only the customer data will be returned to the customer but also the software support in question will be terminated, thus the customers will be faced with the risk of not being able to view and edit their own data. Therefore, it is of critical importance to include clauses to the cloud service contract that would allow the customer to be able to at least view and edit the existing data.

Especially regarding IaaS contracts, it should be included on the contract that at the expiry of the contract the customer data will be returned to the owner of the data and guarantees should be given that the copies of the returned data will be deleted on cloud storages.

IV. CONCLUSION

This paper has briefly introduced the legal, contractual, economic and pricing issues of cloud computing service models. It is observed that no specific regulations regarding cloud service contracts exist in neither the International Law nor the Turkish Law. As cloud computing is revolutionizing the business domain, it is of utmost significance to develop laws that would regulate and address the requirements in the cloud computing domain. It is seen that legal advances related to cloud computing are results of developments realized in the fields of data privacy and protection. On the other hand, as concrete rules regarding cloud contracts have not been developed extensively yet, court decisions and case law are filling the gap at this point. Contracts in the IT domain, and more specially the cloud service contracts, require a separate and specific regulation as they are concluded in the digital environment but also because exclusive issues arise at the termination of these contracts.

REFERENCES


[34] Leitfaden - Vertragsgestaltung beim Cloud Computing, Kompetenzzentrum Trusted Cloud, 2014.