Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2021 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Cloud Computing and Challenges faced in Existing Legal Structure

Divyaraj Ray[a]

[a]Rajiv Gandhi National University of Law, Patiala, India

Received 27 August 2021; *Accepted* 24 September 2021; *Published* 27 September 2021

"The evolving nature of our capabilities as the human race has always shaped the ways in which we govern ourselves and the different developments that are brought about to keep up with the ever-changing nature of scientific and technological advancements along with social and economic changes that result due to these advancements in these fields. One of the most dynamic fields being technology has had remarkable advancements over the years with new developments like cloud computing, which have a significant impact on legal jurisprudence and practice. Cloud computing though has benefits like cost-efficient and convenient storage for business as well as end-users, it has issues like privacy concerns due to unauthorized access and data breach as well as jurisdictional complications in cases of dispute. This article will discuss such issues as well the challenges in the legal framework in India which exist to protect the end user from crimes cyberspace but which do not directly deal with issues and concerns related to cloud computing."

Keywords: *cluod computing, legal structure, challenges.*

INTRODUCTION

One of the major developments in the internet era is cloud computing which has prompted the growth of e-businesses and therefore, it is important to understand the concept or main idea

behind cloud computing. Cloud computing is a model of convenient and on-demand access and availability to computer resources especially data storage and computing power which is supplied with minimal direct and active management by the user and nominal amount of effort from the service provider[1]. In other words, it is the convenient and easily accessible service that is provided by a cloud service provider to the end-user or organization which is usually a web browser. Large cloud computing networks have functions and infrastructure to store data stationed at multiple locations which are act as data centers.

There are many cloud-based applications that end-users use without knowing as these services are availed via a third party which is usually a corporate or e-business company or popular online applications like Gmail, YouTube, sky Drive and thousands of other applications that people use on daily basis on their phones. The growth of these cloud-based applications and the flexible and convenient nature of cloud computing has lead to its popularity in third-party retailers or vendors as well as the end-users.

The United States National Institute of Standards and Technology (NIST) had released the first and widely acceptable definition of cloud computing by identifying its main characteristics which had been submitted as the U.S Contribution to international standardization and according to this definition, "*cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*" There are three models of cloud computing services which are a software as a service known as (SaaS), infrastructure as a structure known as (IaaS), and Platform as a service known as (PaaS).[2]

The three models have different natures of function as SaaS are online services on demand which do not require the consumer to install software to avail such service. PaaS is an effectively operating system in Cloud which allows the end-user to write applications on websites and this model is considered higher-level software than SaaS. While IaaS is the most

[1] Paul M Schwart, 'Information Privacy in the Cloud' (2013) 161(6) University of Pennsylvania Law Review
[2] Jared Carstensen and others, *Cloud Computing* (IT Governance Publication 2012)

recognized model of cloud computing which basically allows end-user to process and store their data.

Cloud computing provides various benefits to e-business and web browsers who avail cloud computing services such as greater flexibility with the application of projects without the construction of as well as cost management which allows profitable margins for the business. The shift of services to cloud service providers allows the business to concentrate on the actual implementation of projects rather than infrastructure and training of personnel granting flexibility and cost-saving alternatives to them. Some of the commonly used cloud services are Gmail, Google spreadsheet, AWS, and Flexi scale.

CORE ISSUES IN CLOUD COMPUTING

The core issue that arises is due to the nature of the cloud which prohibits the end-user from accessing information about how their stored data is utilized or if such data is accessed by someone unauthorized which poses a significant problem as it compromises the privacy and rights of the end-user availing the services of the business who rely on cloud service providers.

1. Privacy Concerns: The end-user always needs to keep in mind the security issues that come along with such easily accessible and convenient data storage option in form of cloud storage and the major concern lies when sensitive data or confidential documents of a user are shared on a cloud as such data is transmitted to a remote location where the server lies and is stored there, this allows the probability of data breach by an unauthorized third party who can take advantage of the relatively loosely structured framework of cloud computing systems. Moreover, the privacy standards and the various legal measures vary according to the region at which such storage database or server is located, and therefore, there are various jurisdictions that one needs to be aware of as these are different. To provide an easy legal solution to these problems the cloud service providers follow uniform international standards along with the national laws of the region where the servers are located. This is legal framework provides a basic and reasonable security standard which these cloud service

providers adhere to, however, such standards do not guarantee that cloud storage is invulnerable.

The data stored in the cloud can either be kept in encrypted form or unencrypted form. Data encryption which makes it difficult to access data directly provides an added layer of protection from unauthorized parties and therefore keeps such data relatively safer than unencrypted data. For the cloud service providers who store data in unencrypted form, ensure basic reasonable security by using two keys that separate the files into a public segment and private segment wherein the public segment is accessible to all while the private segment is protected by restricting access, however, in both cases, the government can easily access data even if it encrypted or protected from non-private access as there are vulnerabilities within the system that allows the government to seek data for purpose of law enforcement or otherwise. This is possible, through laws which include section 69, 69-B of the Information Technology Act, 2000 which enables the authorized government agencies to lawfully access, intercept and decrypt data stored in the computer device regardless of the attributes of the computer model and section 91 of the Criminal Procedure Code which allows stored data on cloud including sensitive data to be accessed by the government authorities. While these interferences are done through lawful procedures, they can be easily misused by authorities and data can be accessible for purposes that do not strictly pertain to law and order concerns.

2. Cyber Crimes and Cloud Security: Crime in cyberspace has progressed hand in hand with the development of technology and cybercrime has infiltrated all major sectors like banking and financing, postal services, e-retail platforms, and commercial facilities, most of which avail service of the cloud provider and this has been a grave concern for many.

One of the newer forms of cyber-attacks on cloud databases which have been widespread in recent years after the advent of cryptocurrency has been 'Crypto Jacking' which involves illegally penetrating through cloud servers to mine cryptocurrencies like Bitcoin and in order to accomplish this cybercriminals have found newer sophisticated methods to access cloud computing systems and then use the system to extract the cryptocurrencies. Crypto-jacking is very difficult to detect and deal with because the hackers use computing resources of the cloud

system of the end-user which slows down the operation but does not shut it down so it gives the illusion that something is wrong with the computer processing system rather than cloud computing system.

Another type of cybercrime that is most common is data breaches which involve issues of leaks and typically occur when cloud accounts are attacked by cybercriminals who are able to gain unauthorized access to cloud networks or utilize programs to copy and transmit data. Some of the major cyber-attacks on cloud servers containing data pertaining to large companies have taken place in India; these include the hacking incident of the DropBox cloud server in 2012, the Data breach of Yahoo in 2013, Union Bank of India Heist in 2016, Wannacry Ransomware attack in 2017 and Data Theft at Zomato in 2017.

3. Loss of Data: Another serious challenge for the end-user and the cloud service providers in the data loss that can happen due to a variety of reasons as even though the data is not physically stored on a local hard drive, it is stored in a physical location in the database and such storage is still susceptible to system failure and data loss due to technical failure or improper maintenance due to human error of the hardware utilized for such storage.

Moreover, the responsibility of such loss has not been placed on a cloud server or the business through which the end-user is availing these cloud storage service as the cloud service provider follow the shared responsibility model wherein the service provider is responsible for the security of cloud system, however, the end-user will be liable for the information stored in the cloud as the shared responsibility suggest that the service provider that cloud service provider has to ensure security mainly through the infrastructure and framework of the cloud system maintenance and protection while the nature of data stored is the sole responsibility of the end-user which means that in the contingent event of data loss, the service provider does not assume responsibility for compensating for such loss and the company which is entrusted with such data is held liable by the end-user resulting in loss of reputation.

The dependence of the cloud service provider on retailers or vendors which the third party to contract enables the provide service to provide the cloud computing service to the end-user

effectively causes complications which can lead to instances of data loss as well, these include failure on part of the third-party vendor to adhere to the contractual terms and conflict between the third party retailer or vendor and the cloud service provider, put the data of the end-user at potential risk of loss.

4. Non-Negotiable Contracts: The cloud computing contracts which are commonly known as (SLA) are valid contracts that follow the essential conditions of a contract provided under section 10 of the Indian Contract Act, 1872. These contracts, however, have non-negotiable terms or very little probability of the same as these are catered to a huge population and are framed in a very standard manner so as to make it convenient for the end-users or consumers of such services. This is usually referred to as click wrap or click through agreements in which the cloud service provider provides for fixed terms and conditions on electronic media which need to be read and accepted by the user so as to access the service as a whole and the negotiability of given terms and conditions solely depends on the cloud service provider and therefore , flexibility of such agreements is restricted according to the cloud service provider and even though these contracts ask for consent of the user , they end user feels the need to comply to these terms without any changes just to access the cloud service and therefore, it can be called consent only in superficial terms with no other alternative present to the end user at times as the agreements provided by most popular cloud service provider through a third party have the same standardized agreements with basic and non-negotiable terms and conditions which specify that the commercially viable data might be shared to other parties and that in case of failure of data or cyber attack the nature of the data kept on the cloud is the sole responsibility of the user which the users often ignore due while accepting these click wrap agreements thereby effectively compromising their personal data and details.

5. Complications of Jurisdiction in case of dispute: There exist various international as well national laws that attempt to regulate the virtual space including cloud computing services and the related cybercrimes as well as a data breach that take place however, one of the biggest challenges that states face is their enforcement as the multi-location set up of infrastructure of the cloud scatter the jurisdiction across different countries with varying standards for laws on

the same subject matter and in such cases, claims against companies are often conflict-ridden with multiple jurisdictions invoked across the globe.

The local laws and state control are often restricted due to the intra-border setup of these services and can create complications in the case which makes it difficult to adjudicate. Data stored in the cloud across the globe result in multiple jurisdictional claims of the data. For example, if a cloud end-user is accessing their services from India using a cloud which physically based in the US but which has using applications developed in Germany by way of a subcontract[3], then the data stored or created using the cloud is neither physically stored in India nor it is processed in India. In such cases where the cloud service provider has been leveraging services from other service providers via subcontracts, it becomes even more challenging to allocate the actual jurisdiction of the cloud.

To tackle this issue, European Union and Russia have formed localization laws that prohibit the cloud service providers to store or process the data of their citizens outside the physical borders of the country and this law has been strictly implemented to ensure data residency prevents the instances of multi-jurisdictional nature of claims and help with the adjudication process as the data is physically stored within the territory of the country. While in India, the law proscribes extra-territorial jurisdiction which permits the data of citizens to be stored outside of the border of the country and the only condition of enduring that jurisdiction not scattered is the cloud computing contract that state the jurisdiction and the laws governing potential disputes in the SLA or contract. However, this significantly restricts the remedy or action an end-user can take against corporate giants based in other countries and often difficulties in establishing jurisdiction in Indian Courts.

LEGAL FRAMEWORK REGULATING CLOUD IN INDIA

The existing legal framework in India does not provide any specific legislation that can directly regulate the cloud space or storage like the localization laws or the Cloud Act adopted by the European Union, but rather the Information Technology Act,2000 has been formulated

[3] Diva Rai, 'Cloud Computing Issues and Challenges' (*iPleaders*, 2021) <https://blog.ipleaders.in/cloud-computing-issues-and-challenges> accessed 20 August 2021

as a general law which indirectly regulates the cyberspace including cloud along with other provisions and rules provided like Information Technology (Reasonable security practices and procedure and sensitive personal data or information) Rules,2011 and Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules,2013.

Section 43 of the Information Technology Act, 2000 regulates the cloud computing industry in a more direct manner as it specifies that corporate and e-business who employ services of cloud service providers and in turn make these services accessible to the end-user or consumer, especially the ones who process and store sensitive information. [4]If such a corporate entity or body which handles sensitive information or personal data is negligent in maintaining the security standards and reasonable security of such data thereby which causes wrongful loss or wrongful gain to any person, then such corporate body will be liable to pay compensation to any person so affected by way of this section. The Information Technology Rules, 2011 also provide guidelines for the corporate entities which include firstly mandatorily ask for consent for processing and collect such data, secondly, they need to insist that such data is collected for a lawful purpose, thirdly the corporate entity needs to follow and strictly to a privacy policy, fourthly, they need to set out instructions for data retention, fifthly they are required to give the end-users or individuals the right to correct the information and lastly, it imposes restrictions on activities like disclose and data transfer. Moreover, these rules ensure that specific sectors such as banking, healthcare or telecom, etc. follow the data privacy guidelines under their respective sectors.

Furthermore, the Persona Data Protection Bill (PDP) had been introduced in parliament in 2019 which has been drafted on similar lines as the General Data Protection Regulation Act, 2016 enacted by the European Union as legislation to regulate businesses to protect the privacy and personal data of the citizens of the countries part of European Union and as non-compliance of the same by businesses can adversely affect them, they have a higher general

[4] Shubhangi Agarwal, 'Cyber Security in India' (*Lexology*, 2021) <https://www.lexology.com/library/detail.aspx?g=d7b0a465-cc55-48e9-9534-b05bf0c036bd> accessed 20 August 2021

standard with regards to the protection of personal data and security. The Personal Data Protection Bill has certain provisions which directly deal with issues in cloud computing like section 24 of the Act which directs the data fiduciaries to protect sensitive and personal data by placing safeguards that prevent unauthorized access to personal data in the nature of disclosure, modification or destruction, and any other misuse. Also, section 25 deals with the breach of data and places responsibility on entities that collect and store personal data to inform the end-user about any data breach that might take place.

CONCLUSION

The development of technology has provided more convenient and easily accessible methods of storing data through the use of cloud computing and cyberspace which includes the cloud has been recognized to be beneficial while also dangerous and such danger stems from the issue of breach of data, unauthorized access to personal or sensitive data and the rise of newer forms of hacking that can cause financial loss to the bonafide user or authorized user. In India, with the rise of internet accessibility and widespread use of the Internet during the present times of the corona virus pandemic when everyone has to work or attend lectures online and write projects or assignments the scope of storing such data along with other personal and sensitive data has increased tenfold and there is an urgent need for proper and specific legislation that deals with cloud and the cloud service providers.

The information of the citizens of India should not be vulnerable to unauthorized access due to the nature of storage in data centers being located outside India's border and therefore, localization laws similar to the ones enacted by European Union and Russia should be considered by Indians lawmakers. Moreover, the existing laws should be amended to add flexibility to the cloud computing contracts (SLA) so as to provide a certain extent of negotiation on the side of the end-user who often feels complied to comply with all the terms and conditions in order to access the services. Further, the existing legal framework needs to be structured in a way as to make it easier to identify the jurisdiction in case of a dispute which is more feasible for the end-user and does not prima facie put them in a disadvantageous position as most of the time the SLAs specify the jurisdiction with respect to their convenience

and these changes can be gradually introduced through legislation like the Personal Data Protection Bill, 2019 which follow a more sophisticated and focused approach to combat the issue of cybercrime and other privacy concerns like a breach of personal data and unauthorized access.