JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

EXAMINING CLOUD COMPUTING IN INDIA THROUGH THE LENS OF COMPARATIVE ANALYSIS OF THE LEGAL REGIME IN SINGAPORE AND SOUTH KOREA

Ms. Chandrika Tewatia Raj
PhD Scholar, Gujarat National Law University, India, chandrikatewatia@outlook.com

Dr. Nidhi Buch
Assistant Professor of Law, and Head Centre for IPR, Gujarat National Law University, India, nbuch@gnlu.ac.in .

The age of information and the reach of various business organisations have made it necessary for every business to hold extensive and efficient cloud computing facilities to retain its business secrets as well as access to work worldwide. India aspires to be a global cloud hub, however, the absence of an effective regulatory framework continues to be an impediment. Cloud's growth and adoption in India has been 'hazy' due to the absence of data protection laws and cloud guidelines in the country. Considering this, an attempt to evaluate the existing cloud computing regulatory framework in India is undertaken through a comparative study of two jurisdictions in Asia- South Korea and Singapore. The paper begins by introducing the concept and importance of cloud computing. Further, the paper explores the usage and implementation of cloud computing laws in South Korea and Singapore which have emerged as the front-runners in cloud digital technology. Finally, the paper engages in an attempt to refine and comprehend the shortcomings of the Indian cloud laws through the cloud computing laws and initiatives of Singapore and South Korea, and attempts to make recommendations in this regard.

INTRODUCTION

"Cloud computing is the third wave of the digital revolution."
– Lowell McAdam, CEO of Verizon

In this era of multinational corporations, cloud computing has become necessary for a globalized business circle, especially after the COVID-19 pandemic. The access and protection of data of companies having ownership and control in different countries can ideally be done with the help of cloud computing. Cloud Computing is defined as software as a service that provides storage facilities for keeping software that can be accessed through the internet. The United States Chambers of Commerce under the National Institute of Standards and Technology has defined "*cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks,*

Submitted: 15/09/2022 **Accepted**: 17/11/2022

servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [1]

Cloud computing is not exactly a novel concept and has been used in search engines and social networking sites. The vast scale of cloud computing makes it ideal for an environment where IT resources fluctuate rapidly and constantly. Cloud resources are typically used by specific users from a pool shared with other customers for pricing. Other factors that have enabled cloud computing to evolve include the budding growth of virtualisation technology, the advancement in universal high-speed bandwidth, and universal software interoperability standards.

Unlike traditional methods that maintain data on a computer, "in the cloud" data is kept on large servers located elsewhere and maintained by a vendor. Offices that require a large amount of archival documents can use cloud without worrying about updates, complicated back-up requirements, or the need for ever-expanding storage and security. Moreover, data stored in the cloud can be accessed more quickly and efficiently than information maintained on a local network, as long as there is a handy Internet connection.

Client data and work products are stored somewhere outside the firm's direct control, raising potential ethical concerns about whether the confidentiality and security of the information are adequately protected within the mandates of professional conduct. The users have no clarity and are adamant about using these cloud because of a lack of certainty. It raises a concern for clients who distribute or store copyright works on a cloud regarding its infringement because of the opaque nature of the cloud. Cloud service providers (CSP) might collaborate with each other to provide cloud facilities to multiple users. In such a case, the question of authorship in copyright rises. One issue for those seeking to protect and enforce rights to cloud-related technologies is identifying whether the technologies are patentable. Another common fear among cloud users is that information and content may become the intellectual property of the CSP. However, there is no evidence of CSP's making claims to own intellectual property in material uploaded by users to date.

The adoption of cloud computing in India has been very cautious due to reasons which can be attributed to lack of privacy laws, absence of data protection laws, inadequate data security, inappropriate data erasing mechanism, poor watch over data handling, licensing, and jurisdictional issues.[2] Due to such 'hazy' regulations over the cloud, India has not utilized the advantages of cloud computing as other countries with privacy and cloud laws.

Singapore has been touted as one of the critical countries for cloud usage and adoption by the government and businesses in Asia. Singapore is one of the first countries to use the cloud to develop a digital environment in the government sector. Singapore has also enacted the Personal Data Protection Act (PDPA) which applies to CSPs and guidelines on the use of cloud services.

[1] Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing' (2011) 2 National Institute of Trade and Commerce under US Chambers of Commerce <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> accessed 23 October 2021.

[2] Mrs. Gowri Menon, 'Regulatory Issues in Cloud Computing -An Indian Perspective' (2013) Journal of Engineering, Computers & Applied Sciences 18.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

South Korea is the first country in the world to introduce an Act on cloud computing, i.e., Act on the Development of Cloud Computing and Protection of Users. The South Korean government has also released regulations for government sectors to adopt cloud computing within their governance models, giving rise to a 'smart' South Korea.

This paper examines the legal framework for cloud computing in both Singapore and South Korea and includes the steps undertaken by the respective governments to promote cloud computing in their countries. It also briefly outlines the laws relating to the cloud in India. The purpose of the present paper is to outline the cloud laws in the two countries, intending to focus attention on the possibility of further changes in regulation for the cloud in India.

CLOUD COMPUTING LAW IN SINGAPORE: AN OVERVIEW

Singapore is considered a global centre for technology and has been the most appropriate country for most of the world's emerging technologies, making it the appropriate country for the cloud computing industry in Asia. Singapore has a 148% mobile penetration rate and a 188% wireless broadband population rate with one of the fastest local connectivity in the Asia Pacific region, making it a cloud hub.[3] It has topped the Global Smart City Performance Index in 2020, which ranks cities based on economic and technological data and citizens' perceptions of how "smart" their cities are.[4] The index furthermore shows that the citizens of Singapore are open to new technologies like the cloud and, ultimately, balancing the economic and technological dimensions involved.

Singapore is working towards a digital economy and has launched a Digital Economic Framework for Action to achieve its goal of becoming a smart and digitally developed country. Cloud Computing forms an essential part of the digital objectives of the country. The government of Singapore is also favourable towards cloud computing, which can be seen through the two initiatives adopted by them- the formation of the Cyber Security Agency and the Smart Nation Program. The Cyber Security Agency provides a cybersecurity strategy under which cloud adoption is encouraged. The Smart Nation Programme is an initiative to harness information technology, network, and big data to create technology-enabled solutions for increasing the total factor productivity, making the lives of Singaporeans better, and attracting foreign firms. This can only be made possible by businesses as well as citizens supporting cloud-enabled technologies. Under the program, the government has introduced a five-year cloud migration plan where the data including contracts would be transferred from an on-site IT system to a commercial cloud which would speed up and improve the quality of government services. By 2020, more than 150 IT systems classified as 'restricted' have been transferred to a commercial cloud, including the Inland Revenue Interactive Network, which supports tax administration and revenue collection. In 2021, around 870 million dollars' worth of contracts

[3] Jerzy Szlosarek, '3 things that make Singapore an ideal cloud computing hub in Asia-Pacific' (*Singapore Business*, 2016) < https://sbr.com.sg/information-technology/commentary/3-things-make-singapore-ideal-cloud-computing-hub-in-asia-pacific> accessed 16 September 2021.

[4] Earth.org, 'Top 7 Smart Cities in the world' (*Earth.org*, 13 July 2021) <https://earth.org/top-7-smart-cities-in-the-world/> accessed 1 September 2021.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

would be shifted to the commercial cloud.[5] The Government Technology Agency (GovTech) of Singapore has reiterated that commercial clouds can be used to build more citizen-centric services and applications.[6]

It is also one of the first countries in the world to use the digital environment in the government sector, for example, having an electronic health record for every citizen in the country. The government of Singapore has also permitted organisations that have adopted cloud computing to receive a 400 percent tax deduction. This amalgamation of geography, governmental support and cloud performance, connectivity, and adoption has made Singapore the ideal hub for cloud services.

During the pandemic, it is the hybrid cloud approach that had been key to the company's disaster recovery and business continuity efforts.[7] 9 out of 10 Information Technology companies in Singapore have already adopted cloud-based services.[8]

The 2018 BSA Global Cloud Computing Scorecard by the Asia Cloud Computing Association ranked Singapore sixth out of 24 primary digital economies for the legal and regulatory cloud environment which includes the data protection regime. The current data economy generation has mandated the enactment of data protection laws in the country. Singapore's Personal Data Protection Act (PDPA) was passed in 2012 and is one of the veteran laws concerning data protection that have been passed in the world. It is based upon the European Union (EU) ePrivacy Directives which predated the General Data Protection Regulation (GDPR). The Personal Data Protection Act governs the collection, use, disclosure, and care of personal data. The Act is being administered by a special government body i.e. the Personal Data Protection of Singapore. The Act applies to the processing of personal data by organisations in Singapore, even personal data which is collected from overseas and transferred to Singapore. It enables individuals to protect their data and regulate organisations on how they collect, use and disclose this personal information. The PDPA is applied to the processing of all personal data by firms in Singapore as well as a collection of overseas data and using it in Singapore. The organisations must bear responsibility if any service provider violates the PDPA. Hence, the contract between the organisation and the service provider must contain provisions that require the service provider to take adequate measures to adhere to PDPA. Organisations should also introduce a standard operating procedure for these service providers and monitor the service provider's compliance with these procedures as well as PDPA.

[5] Eileen Yu, 'Singapore government pushes on with cloud migration' (*ZD Net*, 24 June 2020) < https://www.zdnet.com/article/singapore-government-pushes-on-with-cloud-migration/> accessed 20 September 2021.

[6] DXC Technology and Dell, 'Boosting Singapore's Smart Nation goals with the cloud' (*GovInsider*, 15 March 2021) <https://govinsider.asia/resilience/dell-dxc-boosting-singapores-smart-nation-goals-with-the-cloud/ > accessed 28 September 2021.

[7] Alibaba, 'Survey Finds Over 70% of Asian Businesses Favor Asian Providers' (*Alibaba Cloud*, 26 January 2021) < https://www.alibabacloud.com/blog/survey-finds-over-70%25-of-asian-businesses-favor-asian-providers_597215> accessed 1 October 2021.

[8] Aaron Tan, 'Singapore tops cloud adoption in ASEAN' (*Computer Weekly*, 8 February 2021) <https://www.computerweekly.com/news/252495974/Singapore-tops-cloud-adoption-in-ASEAN> accessed 4 October 2021.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Organisations that are handling and controlling personal data must comply with the following obligations.

- **Accountability**

Organisations must adhere to obligations under the PDPA and provide information about data protection policies, practices, procedures for filing complaints, designating a Data Protection Officer whose credentials are available to the public. The organisation is held responsible for its activities by regulatory bodies, businesses, and individuals whose data is stored with these organisations.

- **Notification**

Individuals or businesses must be informed of the reason for the organization's collection, use, and disclosure of their data.

- **Consent**

The organisation can only collect, use and disclose data for the purpose for which the individual has given consent. The individual is allowed to withdraw consent and the organisation must inform them of the consequences of withdrawal and cease to use, collect and disclose that individual's data.

- **Purpose Limitation**

The organisation must use personal data which would be considered appropriate under circumstances by a reasonable person. The organisation cannot force an individual to give consent for disclosing his data as a requisite for providing a product or a service.

- **Accuracy**

The organisation must ensure that the collected data is accurate and complete, primarily when the data is used to make a decision affecting the individual or used by another organisation.

- **Protection**

The organisation must undertake reasonable security measures to prevent unauthorised access, collection, use, or disclosure of data.

- **Retention Limitation**

The organisation must stop retaining any data and dispose it properly if it is no longer required for business purpose.

- **Transfer Limitation**

Organisations can only transfer data to another country if the stand of protection can be compared to that of PDPA.

- **Access and Correction**

Individuals can request access to their data as well as information on how the data was used and disclosed in a year before the request has been made. If there is any correction in the data provided by the individual, the organisation must correct the data as soon as possible and send the corrected data to other organisations to whom this personal data had been disclosed within a year before the correction was made.

- **Data Breach Notification**

An organisation must take steps to notify the individuals, in the case of a data breach. If the data breach has resulted in significant damage to the individuals, then the organisation must

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

notify the PDPC and the affected individuals as soon as possible.

- **Data Portability**

The individual can request his data to be transmitted from one organisation's possession and control to another organisation in a commonly used machine-readable format.

The above obligations would also apply to data that is stored in a cloud. Concerning the cloud, the PDPC has released guidelines on the use of cloud services on 9 October 2019. PDPC has revised the Advisory Guidelines on the PDPA to include cloud service providers (CSP) which are processing personal data to have a secure environment for data protection. The new guidelines will help businesses and CSPs understand their obligations under Singapore's data protection regime. According to Philip Heah of Infocomm Media Development Authority (IMDA), the guidelines have been drafted to focus upon data that is transferred across the world that would be protected.[9] The new guidelines would also clarify how organisations can comply with PDPA through the selection of a CSP that would be able to provide the essential requirements for the protection of personal data.

CSPs would be considered to be data intermediaries which only process personal data on behalf and for their customers, subject to the protection and retention limitation obligations as given above. An organisation that is working as a data intermediary must comply with restrictions on the transfer of personal data outside Singapore i.e. the Transfer Limitation Obligation. The CSP must ensure that the place/country where data is being transferred has a data protection regime having the same force and enforceability as the PDPA. The organisations need to make sure that there are legally enforceable obligations present within the country/place where the data has been transferred. A written contract between the CSP and the user can be considered to ensure that there are legally enforceable obligations. The contract should deal with the standard of protection and the overseas locations where personal data might be transferred. According to the Personal Data Protection Regulations 2014, the contract must outline all jurisdictions where the data might be transferred. But it is challenging to apply the same rule to CSP and their contract with the user as they might not be able to state the location where the CSP might transfer the data and is generally left at the discretion of the CSP. Hence, in this case, the cloud service user can take the following appropriate steps:

i. The CSP in Singapore has met the relevant marketing standards such as ISO 27001 etc.
ii. The CSP who have transferred their data overseas must reassure the users that they have followed all standards like producing audit reports upon request.[10]

In the event of a data breach, the onus is upon the cloud user i.e. the party who has transferred the data to ensure that the CSP chosen by them offers sufficient protection for the data which had been transferred. The cloud user's due diligence in choosing the CSP, as well as the

[9] Aaron Tan, 'PDPC issues cross-border data transfer guidelines for cloud services' (*Computer Weekly*, 14 October 2019) <https://www.computerweekly.com/news/252472226/PDPC-issues-cross-border-data-transfer-guidelines-for-cloud-services > accessed 25 October 2021.

[10] Mark Robinson, Peggy Chow, 'Singapore issues guidance for cloud services' (*Lexology*, 14 November 2019) <https://www.lexology.com/library/detail.aspx?g=4695ca40-8f43-4cb7-b236-dea90ff711da> accessed 20 October 2019.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

locations and sub-processors, would be taken into consideration while determining the liability of the CSP.

Other than the PDPC which has introduced guidelines for CSP, several standards relating to cloud computing security have also been developed. In 2012, a technical reference for the virtual security of servers was introduced which was followed by the world's first standard for cloud security in 2013. Later in 2014, an accredited certification scheme was also introduced which has become the essential and actual standard for the cloud computing industry in Singapore. This is known as the Singapore Standard or MTCS (Multi-Tier Cloud Security Certification Scheme) which has been developed by the Information Technology Standards Committee (ITSC). MTCS covers multiple tiers of cloud security and encourages the adoption of comprehensive risk management and security practices. In 2018, guidelines for cloud outage incident response (COIR) were released which focus upon business continuity as well as disaster recovery management. These guidelines will help to understand how to respond to a cloud outage and ultimately strengthen the trust and reliability of the CSPs. The main objective of these guidelines is to reduce and mitigate any damage or loss caused by cloud outage by choosing the appropriate protection measures for their business continuity. Cloud outage can be associated with operational mistakes, system failure, and natural causes such as floods and fire, but do not include outages caused by lapses in cyber security or malicious acts. The adoption of the COIR guidelines is voluntary for the CSPs. Even then, they are encouraged to disclose their service support in case of a cloud outage to the ITSC. Now, the technical reference for the security of servers has been enhanced as an international standard (ISO/IEC 21878:2018).[11]

An online survey had been conducted for organisations in Singapore and their adoption of the cloud within their industry considering the risks and the potential of cloud computing for their business.[12] Organisational executives who could take decisions about the adoption of cloud computing in their companies answered the survey. As a result of the survey, it was found that even in the year 2020, the adoption of cloud computing can be seen in a nascent stage but the attitude of organisations towards the technology, observed advantages can be seen positively in the adoption of cloud computing in Singapore.

SOUTH KOREA'S CLOUD COMPUTING REGIME

Commented [N1]: Logical sequence is missing

South Korea became one of the first countries in the world that has introduced a law on cloud computing. The cloud-specific law shows that South Korea is focused on boosting the cloud industry in the country. The cloud computing industry in South Korea is expected to double from the current US$1.5 billion, where the SaaS model of cloud accounts for 45% of the

[11] Infocomm Media Development Authority, 'Cloud Computing and Services' (*IMDA*) <https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Cloud-Computing-and-Services> accessed 28 October 2021.

[12] Margaret Tan, Trisha T. C. Lin, 'Moving Forward with Future Technologies: Opening a Platform for All' (19th Biennial Conference of the International Telecommunications Society: "Moving Forward with Future Technologies: Opening a Platform for All" Bangkok, Thailand, 18th-21th November 2012) < https://www.econstor.eu/handle/10419/72509> accessed 1 November 2021.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

market.[13] Digital native businesses along with media and gaming companies are the major spenders in the industry. Other industries including E-commerce industries are also tapping into big data which helped them provide personalized services to their customers. The 'chaebols' or individual massive corporations are also creating their private cloud which may encourage further cloud adoption in the country. Large corporations have already begun the move to transfer their data into a public cloud from data centre applications.[14] The sudden COVID-19 outbreak has also augmented the demand for cloud as several IT companies have adopted the work from home model through the cloud. According to a report on Global Data, Market Opportunity Forecasts to 2025: ICT in South Korea, adoption of technologies like Artificial Intelligence (AI), Internet of Things, and Big Data is on the rise as a part of Digital Transformation to improve the efficiency of services, gain advantages and encourage enterprises to upgrade their technology infrastructure. If the CSPs continue to introduce products at the present rate and the stance of the Korean government doesn't change then the overall impact is realized to be 54 trillion Korean won.[15]

The earlier regulations did not allow government institutions to use any infrastructure other than the private government cloud i.e. G-Cloud. In 2018, new regulations 'Basic Plan for Cloud Computing Promotion in the Public Sector' was released which allowed the government to expand the number of public sector institutions that can use the cloud (hybrid or public), ultimately achieving the goal of smart cities. The regulations also focused on a cloud environment solely dedicated to the government and using cloud services for applying Big Data and AI to government services. The Government of South Korea focused on shifting all its government services to the cloud leading to A savings of $32 million. Hence, the current government cloud service would be based on a SaaS model rather than the earlier Infrastructure as a service (IaaS) model. The conversion of data centres into cloud centres would start with the Government Integrated Data Center in Daegu[16] through the introduction of a dedicated cloud portal i.e. the K-ICT Cloud Innovation Center. In June 2020, the president of South Korea Moon Jae In declared the Digital New Deal which proposed a transition to a digital economy by digitalizing the national infrastructure while promoting DNA- data, network, and AI. The Korean Association of Cloud Industry provides data and studies relating to cloud computing on its website.

Many South Korean industries were reluctant to invest in cloud services or store their data in cloud as they were cynical of the safety of the data being stored. The companies were fearful

[13] Mark Bowen, 'Enterprise server spending in South Korea predicted to increase' (*Intelligent CIO*, 4 October 2021) <https://www.intelligentcio.com/apac/2021/10/04/enterprise-server-spending-in-south-korea-predicted-to-increase/#> accessed 2 November 2021.

[14] iMarc, 'South Korea Cloud Computing Market: Industry Trends, Share, Size, Growth, Opportunity and Forecast 2021-2026' (*iMarc*) <https://www.imarcgroup.com/south-korea-cloud-computing-market> accessed 15 November 2021.

[15] Boston Consulting Group, 'South Korea's Market Report' (*BCG*) < https://www.bcg.com/en-in/publications/2019/economic-impact-public-cloud-apac/south-korea> accessed 14 November 2021.

[16] Kim and Chang, 'Korean Government Announces Cloud Computing Promotion Plan, Repealing the "Information Classification System"' (*Kim and Chang*, 21 September 2018) <https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=20563> accessed 19 November 2021.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

of losing information or mismanagement of data by the domestic as well as foreign CSPs. Most of the CSPs that were present in Korea were mostly of foreign origin which made the companies, even more reluctant as the data could have been stolen by foreign rivals or competitors. The laws that regulated confidential information in South Korea had several discrepancies which were not adequate. Hence, the government decided to come up with- The Act on the Development of Cloud Computing and Protection of Users (Cloud Computing Act) which promotes and develops cloud computing, cloud computing technology, and cloud computing service.[17]

According to the Cloud Computing Act, an agreement between the CSP and the user will be deemed to satisfy the requirement of an IT facility, device, and system that is essential to obtain a permit or approvals under other laws. The Act contains a system of procedures that directly or indirectly limit cloud computing in industry-specific laws and privacy laws of Korea. It does not contain any explicit prohibitions and hence, adopts a negative regulatory framework where cloud computing is allowed unless expressly constrained by another statute. Some of the features of the Cloud Computing Act are as follows:

- It is not necessary for companies using other companies' cloud services to have their own computing facilities within their place of business, to be eligible to obtain business license and permits (Article 21). Hence, the companies will find it more cost effective and less time consuming to obtain these licenses.
- The Cloud Computing Act includes the same stipulations about the protection of data stored in cloud which have been included in the Personal Information Protection Act (PIPA) and the Act on Promotion of Information and Communications Network Utilization and Information Protection (Article 4).
- In the event of a cybersecurity incident or data leak, CSPs must notify users. In case of a cloud data leakage, the Minister of Science, Information and Communications Technology and Future Planning (SIP) must be informed as well (Article 25).
- Users can demand the names of the countries where their cloud data is stored from the CSPs. The minister of SIP may also ask the cloud information stored in that country to be provided to the users, if necessary (Article 26).
- Cloud data must not be provided to third parties by the CSPs. After the expiry of the service agreement between the CSP and the user, the data which is stored in the cloud must be returned to the user or must be destroyed if the data cannot be returned (Article 27).
- Because of the Cloud Computing Act, financial institutions do not require to a cloud computing facility to process their data as they are now allowed to outsource the processing of data to domestic and foreign CSPs. But certain amendments in other acts like PIPA, Use and

[17] Republic of Korea, 'Act on the Development of Cloud Computing and Protection of Its Users' (September 2015) <https://www.law.go.kr/LSW/lsInfoP.do?chrClsCd=010202&lsiSeq=169562&viewCls=engLsInfoR&urlMode=engLsInfoR&lsId=012266#0000> accessed 24 September 2021.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

Protection of Credit Information Act are required for the protection of personal credit information data stored in clouds.[18]

- The government can promote the international exchange of cloud computing related information, cloud computing exhibits, joint research and development of cloud computing with other countries and cooperation between countries for enhanced efficiency of cloud computing services.
- A CSP is subject to criminal penalties if the data is provided to a third party without the consent of the user of the cloud. The failure to notify the user and the authorities about the data breach or destroying or returning information would also be subject to a fine.

According to the Act, the government must make efforts to adopt cloud computing and recommend using private companies' cloud models. In support of this, the 2018 regulation had been released which has already been discussed by the author.

The interplay of PIPA and the Network Act plays a significant role in the implementation of the Cloud Computing Act in South Korea. The government has enacted both the acts to protect the privacy and security of the citizen and their personal information. Both acts apply to CSPs in terms of data privacy, which require the user's prior consent for collection, use, and disclosure of personal information. The CSP using this personal information must take stringent measures to ensure that there is no loss, theft, or leakage of personal information.[19] If there is any data breach due to lack of security measure under PIPA or the Network Act, then the CSP might be subject to a criminal penalty of not more than two years imprisonment or a fine of not more than 20 million Korean Won (Article 73 of PIPA and Article 73 of the Network Act).[20] According to Article 17 (3) of PIPA, if the personal information manager which can be construed as a CSP, is providing the personal information to a third party then the user must be notified and his consent must be obtained while concerning the trans-border transfer of personal information. In January 2014, Google was fined 212 million won under this Article for collecting the personal information of South Korean citizens without their consent.[21]

The biggest obstacle to the proliferation of the cloud computing industry in South Korea is the stringent data privacy laws. Under PIPA and the Network Act, cloud computing is considered to be a data processing unit and hence, requires compliance with strict regulation regarding delegation of power of data storage to a third party. This strict compliance is not compatible

[18] Kwang Bae Park and Hwan Kyoung Ko, 'South Korea's New Cloud Computing Act and New Rules on Outsourcing of Data Processing by Financial Institutions' (*Bloomberg Law*, 18 September 2015) <https://news.bloomberglaw.com/privacy-and-data-security/south-koreas-new-cloud-computing-act-and-new-rules-on-outsourcing-of-data-processing-by-financial-institutions> accessed 17 November 2021.

[19] Seungmin Jung, Young-Hee Jo and Youngju Kim, 'Q&A: cloud computing law in South Korea' (*Lexology*, 13 November 2021) <https://www.lexology.com/library/detail.aspx?g=c52a592e-ee24-490e-b611-3388aff41236> accessed 10 November 2021.

[20] Seungmin Jung, Young-Hee Jo and Youngju Kim, 'Cloud computing in South Korea' (*Lexology*, 18 November 2021) <https://www.lexology.com/library/detail.aspx?g=cbdef3bc-6cd5-46fa-b86e-e1a5f212c8e6> accessed 10 November 2021.

[21] Julia Yoon, 'South Korean Data Localization: Shaped by Conflict' (*University of Washington*, 28 February 2018) <https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/> accessed 23 November 2021.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

with the very nature of cloud computing and hence makes the companies reluctant to adopt cloud computing. Till now, there has been a lack of clarity on whether the present Cloud Computing Act would prevail over PIPA and the Network Act which might lead to extensive acceptance of cloud computing within South Korea. As South Korea is still at war with North Korea, there must be a stringent data localization policy where strict management of location information and spatial data would provide security. Hence, South Korea's economy needs to maintain a balance between cross-border data flow and data localization.

EVALUATING INDIAN LAWS FOR CLOUD COMPUTING

The Indian Cloud Computing sector has been estimated at US$2.5 billion in 2018 and has a host of small CSPs as well as major CSPs in the world, namely Amazon, Microsoft, Google, and IBM. The Government of India has also introduced an initiative to implement and accelerate the delivery of government e-services by introducing a GI Cloud called as MeghRaj.[22] This will increase the dissemination of the usage of cloud in India alongside subsidising the spending of the government on information technology. There are no government initiatives or policies that provide incentives to the enterprises in the cloud computing industry.

At present, there is no law regulating cloud computing services in India. There is also a lack of data protection laws which has led to the indirect application of various laws to the cloud computing sector. CSPs do not require any local licence or incorporate any lawful body to offer cloud services. The services may even be allowed on a cross-border basis without restrictions on the foreign investment used to set it up. Only an incorporated body in India offering cloud services would be subject to certain compliances like labour law, goods and service tax, corporate, etc.

The CSPs in India are subject to various laws and rules indirectly. The Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 regulate the collection, receipt, possession, storage, handling and transfer of personal information of natural persons in India.[23] These rules apply to any data processor who is collecting data and hence, CSPs may also fall within this category as they also collect data and process information. According to the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, the Indian government can intercept, monitor or decrypt information that is generated, stored or transmitted on any computer resource in case of state security and law enforcement. CSPs may also be protected as intermediaries under the Information Technology (Intermediaries Guidelines) Rules 2011. Typically, the term

[22] National Informatics Centre, 'About NIC' (*Cloud.gov.in*) <https://cloud.gov.in/about.php> accessed 18 September 2021.

[23] Section 43A of Information Technology Act- Compensation for failure to protect data. -Where a body corporate, possessing, dealing, or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

"intermediary" is used for internet service providers or network service providers who facilitate the use of internet and grant access to third party content. Even though CSPs do not provide such services, they can be understood as intermediaries in a broader sense. Intermediaries have several compliance requirements and may enjoy safe harbour protection for third party information. The Information Technology Act has extra-territorial jurisdiction and hence, CSPs committing any contraventions outside India might also be penalised.[24] An amendment to the guidelines relating to intermediaries will allow monitoring of unlawful information and removing it as well. It also suggested a compulsory provision for intermediaries having 50 lakh users to have an Indian establishment. But, alas, they also lack the force of law.

In 2012, the Ministry of Electronics and Information technology described certain aspects of cloud computing under the National Telecom Policy for the first time.[25] The Telecom Regulatory Authority of India (TRAI) released a consultation paper on cloud computing in 2016 and asked for recommendations on the same in 2017 and 2019 respectively. TRAI had recommended a self-regulatory framework for CSPs where a separate body framework must be set up, industry codes for quality of service parameter, a dispute resolution framework and requirements for billing etc. However, these have no force of power and hence, there is still a lack of regulation in the cloud computing sector.

The Personal Data Protection Bill, 2019 has also been introduced by the Indian government to substantiate the existing privacy framework in India.[26] According to the bill, the data processors need to implement specific security standards, transparency and accountability measures while entering into a contract with customers. There is also another ongoing recommendation concerning laws for the protection of non-personal data, i.e. data that is anonymous or cannot be connected to an identifiable person. An expert committee has been set up which has recommended separate legislation to govern non-personal data and an independent body for its regulation.[27] Due to the lack of effective regulation as well as development in the cloud computing sector, it is imperative that a better and different legal framework be introduced rather than the indirect application of pre-existing laws.

CONCLUSION: ROADMAP TO THE FUTURE OF CLOUD COMPUTING IN INDIA

The remarkable advancement in technology has brought this cloud computing sphere to a boom, especially during this pandemic. Cloud computing was being indirectly justified in India

[24] Vikram Jeet Singh, 'Cloud Computing In India - The State of Play And What's Next' (*BTG Legal*, 2 November 2020) < https://www.btg-legal.com/post/cloud-computing-in-india-the-state-of-play-and-what-s-next?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration> accessed 4 October 2021.

[25] The Centre for Internet and Society, ' National Telecom Policy, 2012' (*CIS*) < https://cis-india.org/telecom/resources/national-telecom-policy-2012#:~:text=The%20National%20Telecom%20Policy%2C%202012,inclusive%20socio%2Deconomic%20development%E2%80%9D> accessed 29 November 2021.

[26] PRS Legislative Researcher, 'The Personal Data Protection Bill, 2019' (*PRS India*) <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019> accessed 14 September 2021.

[27] Vidushi Marda, 'Non-personal data: the case of the Indian Data Protection Bill, definitions and assumptions' (*Ada Lovelace Institute*, 15 October 2020) <https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/> accessed 10 November 2021.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

through pre-existing laws, but with the rise of regulations in other countries, India must also couple with the application of laws that need adjustment to meet the current needs and standards.

The Indian government has not taken any initiatives in terms of development of cloud computing by introduction of incentivising through taxes or any policies unlike Singapore and South Korea. Even though all three countries have started the adoption of a government cloud and the transfer of government e-services to this cloud, there needs to be a better percolation of cloud computing services in India. Programs for the effective usage of cloud computing in the public sector and the effect dripping into the economy must be introduced, similar to the Digital Economic Framework for Action of Singapore and the Basic Plan for Cloud Computing Promotion in the Public Sector in South Korea.

Singapore's PDPA based on the GDPR guidelines has introduced compliances and SOPs for CSPs while PIPA of South Korea also enumerates stringent measures that the CSP must take in case of any personal data loss and even provides for punishment. On the other hand, India is still in the process of finalising the PDPA which has also led to CSPs and their users being completely vulnerable. The compliance for Singapore as well as South Korea are common standards as most of them have been based upon the GDPR. The Indian government must introduce obligations for data storage with CSPs like accountability, data portability etc. The absence of such obligations has led to a vague and ambiguous environment for the cloud computing industry. India should also introduce procedures for cloud security and encourage the adoption of comprehensive risk management and security practises like Singapore has introduced. These can be introduced as voluntary guidelines by the government for the CSPs to adopt in the event of a data outage.

India can learn from the unique Cloud Act of South Korea and introduce a law relating to cloud computing or rules in addition to the Information Technology Act 2000. The negative regulatory framework followed by Korea might be an appropriate mechanism for regulating cloud computing in India as well. Singapore has adopted various guidelines within PDPA as well as compliances for CSPs but the author suggests embracing a framework like South Korea would be more feasible for India.

Currently, there are no penalties for a CSP in the event of a data breach, making the users using these cloud vulnerable due to unidentified or non-consenting individuals accessing their personal or confidential data. Following the example of South Korea, a criminal penalty along with the guidelines must be introduced to keep in check data breaches.

The government's efforts to promote cloud computing and its implementation within Indian jurisdiction, guidelines for CSPs, obligations for data storage, punishment for a data breach should form the basis of effective implementation, promotion and adoption of cloud computing in India. It is pertinent to note that cloud computing can be understood as the most important and critical technology used in most areas, especially during this pandemic, which has completely changed the way organisations operate and work. Henceforth, the Indian government needs to introduce guidelines, laws, rules or regulations for cloud computing for effective adoption of cloud computing as it has transpired in South Korea and Singapore. India

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/

needs to take charge in the cloud sector to achieve its goal of being a smart nation. India must realise that cloud computing is computing for the masses, which offers the latest technology while leveling the playing field more than ever before.[28]

[28] Douglas R. Holschuh and David C. Caverly, 'Techtalk: Cloud Computing and Developmental Education' (2010) Journal of Developmental Education, Vol. 33, No. 3.

Copyright © 2022. Journal of Northeastern University. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://dbdxxb.cn/