CHAPTER 2

PRIVACY IN CLOUD COMPUTING: A COMPREHENSIVE STUDY OF DATA PROTECTION LAWS

Shashank Rai, Ms. Ankit Paul Kaur

Fifth-Year B.A. LL.B (Hons.), Lovely Professional University, Phagwara, Punjab. shashankraicoc@gmail.com

Assistant Professor, Lovely Professional University, Phagwara, Punjab. ankit.27861@lpu.co.in

Abstract

Cloud computing is all about resource sharing and direct access to the nebula of computers that store trillions of bits of information. Businesses and governments have stored our data in databases since the 1960s, when information technology capabilities expanded. Using the cloud implies giving up some control to a third party, no matter how careful a person is with their personal information. Databases may be searched, altered, and cross-referenced, and their data can be shared with organizations worldwide. Governments worldwide are significantly changing policies and infrastructure to enable economic opportunity, attract international investment, safeguard society's security, and improve institutions. Our devices and infrastructure are being built with information-gathering in mind. Individuals' ability to govern how data about their life is transmitted and analyzed is becoming extremely limited. The cooperation and mutual trust of the service providers and infrastructure providers will play a critical role in data security. We are not prepared for the future that has already taken shape. Our laws are unable to handle these dangers at this time. Our technologies are unsecure and expose personal information. The main idea of this paper is to analyze what cloud computing is and in the light of right to privacy which has been recognized as a fundamental right, explore the complexities of data leakage, data processing and privacy laws by comprehensive analysis of data protection regulations in various nations.

Keywords: *Cloud Computing, Personal Information, Privacy*, *Data Leakage, Data Processing, Data Protection Law*

LIST OF ABBREVIATIONS

AWS	Amazon Web Services

E.U.	European Union
GDPR	General Data Protection Regulation
H.P.	Hewlett Packard
I.T.	Information Technology
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
KYC	Know Your Customer
PaaS	Platform as a Service
PDPB	Personal Data Protection Bill
SaaS	Software as a Service
VC	Virtual Computers
VPN	Virtual Private Network

1. INTRODUCTION

Cloud computing refers to a computing model in which processing is shifted from individual computers or application servers to a network of computers. Cloud users have to worry about their computing demands because all underlying complexities are concealed. Cloud computing enables on-demand access to a vast pool of dynamically scaled and virtual resources.

A cloud's services are not restricted to using online apps; they may also provide I.T. administration services like requesting a software stack, system, or web appliance. Storage, servers, databases, networks, software, and other resources are all part of a cloud. As a result, cloud computing is defined as distributing

applications, infrastructure, and platforms as a package over the internet. These subscription-based applications may be accessed from an internet browser, so consumers do not have to worry about the service provider's system or where the software and data are stored on the servers. Cloud computing is famous for various reasons, including the fact that it provides storage capacity above the conventional limit and saves computer expenditures.

Outsourcing data storage and administration is the primary difficulty of cloud computing. People utilize cloud services unknowingly through e-mails, remote storage services, social media, backup services, and so on. They have no clue where their data is kept geographically, who has access to it, who retains it, or what happens when they ask to delete the same. In general, privacy concerns are not new. In the cloud computing context, privacy concerns are becoming increasingly dangerous. As a result, these regulations may not be appropriate in such a dynamic and public setting, and they will need to be tailored to address all privacy concerns. However, there is no certainty that these rules will be enforced in the cloud. Different roles in the cloud value chain can propagate and regulate privacy and security risks while utilizing cloud services: providing platform and services, software, intermediate and end-users of cloud services, and so on.

However, the legislation across the globe is continuously attempting to cope with the ever-expanding trend of Information Technology. Then again, for the attempt made by the legislature, technology appears to be way ahead. It has progressed so rapidly that regulatory authorities seem to never be able to compete with it. The fact is that legislature of other jurisdictions is now employing digital signals to monitor our day-to-day work. It tracks our digital footprints by analyzing the information we post on the internet. Our personal information is not private; our e-mail addresses are being shared with internet service providers, our online searches are shared with firms, and our cellphone conversations are shared with telecom companies. In today's world, our data is not only our government or any other organization that has access to our personal information, including bills payment details. In the worst case, they even have access to our credit or debit cards information and bank account details. In the case where these data are not adequately managed by legislation, they will have access to each and every data that we desire to keep private without a legal warrant. As privacy tends to be a necessary prerequisite for democracy to work, and if the government does not allow individuals to act freely, it effectively undermines the concept of democracy.

As a result, both the public and commercial sectors collect and exploit personal data on a massive scale and for various objectives. While data can be helpful, the uncontrolled and indiscriminate use of personal information has generated worries about an individual's privacy and autonomy. Some concerns center on database centralization, individual profiling, more excellent monitoring, and the resulting erosion of human autonomy. Hon'ble Supreme Court's historic decision in aadhaar case by nine judges' bench, came up with a reasoning that the concept of privacy is an integral fragment of human life; hence, under the Constitution of India it is considered as a fundamental right. When it comes to personal data protection and right to privacy, both are said to be inextricably linked; both aim to protect comparable concepts, such as an individual's independence and dignity.

On 31st July 2017, the government established a Committee on Data Protection, which is headed by Justice B.N. Srikrishna. It was given the task of evaluating the critical concept of data leakage problems. The Personal Data Protection Bill of 2018 was developed by a committee led by Justice B.N. Srikrishna and some proposals and recommendations were made based on it. The enactment of the abovementioned Bill, namely, the Protection of Personal Data Bill, 2019, was set in motion based on the recommendations stated in the committee's report and proposals received from various stakeholders. The Bill's primary goal is to create a reliable and straightforward personal data protection framework for India.

The concept of right to privacy in addition to personal data protection stands not the same in terms of wording and extent. The right to privacy entails a blanket restriction on interfering with one's private life, subject to specified public interest standards that may allow intervention in some circumstances. Whereas the personal data protection is considered to be a current and active right, with checks and balances to safeguard persons where their information is to be processed. Also, processing of private data is considered as a critical element of personal data protection, including independent oversight and honor for the individuals' rights.

2. CLOUD COMPUTING EVOLUTION

The concept of cloud computing is said to have emerged around the 1950s-60s. The Foundation block for the same is set to be kept by IBM, who, for the first time, introduced the concept of virtual computers (hereinafter referred as V.C.) around the 1970s. The concept of V.C. is simple yet technical to understand; to put it simply, a V.C. can be defined as a software computer that does working like a real computer, which has the capacity to run an operating system and programs installed into it. The V.C. is programmed in such a way that the actual resource files are with the host. Every V.C. has the capacity to perform the exact same functions as a regular computer will do. However, more onto that, it provides extra benefits like mobility, easy management, and additional security. When IBM released its first V.C., customers could operate their computers on hardware maintained and controlled by the host.

In the 1990s, when telecommunications businesses switched from point-to-point data connections to Virtual Private Networks (hereinafter referred as VPN), the concept of cloud computing truly gained popularity. During the 1980s computer boom, several industries were seeking a means to connect all of their computers being operated under a single roof to be associated with each other so that they could have easy access to each other's shared data, and here in this case VPNs enabled them to do so. You could tell that the cloud would take off when the price dropped and the service improved.

In 1999, Salesforce.com became a cloud computing pioneer by providing business applications through a simple website. Any client with an Internet connection may access the apps, and businesses could acquire the service cost-effectively.

Microsoft debuted the Azure cloud application platform in 2008. People can use cloud apps to exchange data via the internet, and for the reason that they are on the cloud, they do not require any additional storage

space on their computers or devices. Anyone having access to the internet may utilize these programmes. Microsoft Azure provides users with the ability to host websites, manage their data, and much more.

Google Play joined this race in 2009 by offering Cloud Computing Enterprise Applications. As soon as other organizations became aware of the advent of cloud computing, they started offering their cloud services. Following that, other firms such as H.P., IBM, Oracle, and Alibaba announced their Cloud Services. Following its announcement in 2011, H.P. entered the "cloud wars" in 2012 by introducing a public beta of 'H.P. Public Cloud.' OpenStack was used to deliver storage and Content Delivery Network services through the service. In 2012, another H.P. business unit (The Converged Cloud Unit) unveiled 'H.P. Converged Cloud,' which offered private, managed, and public cloud choices. In 2013, the two business divisions and clouds united.

Satya Nadella took over as CEO of Microsoft in February 2014, succeeding Steve Ballmer. This was a watershed moment for Microsoft and its cloud division, working diligently to catch up to Amazon. Satya was a driving force behind Microsoft's shift to cloud computing before he became CEO, and he has continued to place a strong emphasis on the cloud since then. In 2014, Satya described his cloud-first strategy in his first letter to staff. Microsoft's technique was incredibly effective.

After recognizing it would be nearly impossible to compete with Google, Amazon, and Microsoft, a few cloud suppliers opted to close their public IaaS clouds in 2016. Verizon said in February that it would discontinue its Public Cloud products, while H.P. announced in October that it would stop its H.P. Helion Cloud and instead work with public cloud suppliers.

Amazon made a couple of purchases in 2019 to assist clients in migrating to its cloud. Amazon revealed in January that it had purchased Cloud Endure, an Israeli business focusing on cloud disaster recovery, for $200 million, as well as TSO Logic. This startup was working on cost analysis to compare cloud and on-premises expenses.

As we reflect on the history of cloud computing, it is clear that this area, which was the enabler of digital transformation for many enterprises, underwent its evolution over time. And this is only the start; the greatest is yet to come.

3. CLOUD COMPUTING CLASSIFICATIONS

3.1. Public Cloud

The public cloud model, one of the most common cloud computing platforms, allows organizations to host their applications or consume services on a public cloud. This I.T. approach offers on-demand computing resources controlled by a third-party service provider and used by several enterprises. Cloud computing service providers divide their infrastructure into virtual machines, often provided to businesses on a pay-per-use basis. This strategy may be utilized efficiently by enterprises to manage traffic spikes.

3.2. Private Cloud

A private cloud approach is better ideal for organizations with compliance or storage constraints for keeping data on the public cloud. Businesses may centrally consolidate I.T. resources in a private cloud and enable dynamic provisioning and de-provisioning via a centralized portal. This private cloud is exclusively available to customers from a single firm or set of organizations, and the organization can tailor the private cloud to its own needs.

3.3. Hybrid Cloud

It allows businesses to reap the benefits of both private and public cloud computing technologies. When an enterprise's internal I.T. capacity is wholly used, for example, the public cloud model might be used to accommodate the additional demand. The hybrid cloud architecture is also preferable for hosting workloads that must meet compliance or data security standards.

4. CLOUD COMPUTING SERVICES

4.1. Infrastructure as a Service (IaaS)

IaaS enables individuals to use infrastructure on a pay-as-you-go basis. Infrastructure comprises development tools, operating systems, servers, networking firewall, and storage.

4.2. Platform as a Service (PaaS)

PaaS is often used to launch apps. It provides individuals with a comprehensive infrastructure configuration that includes a database, development tools, middleware, servers, storage, and networking. Developers, for example, can utilize a PaaS provider's framework to design and configure cloud-based apps and use in-built software components.

4.3. Software as a Service (SaaS)

Individuals can access software products using the SaaS model on a pay-per-use or subscription basis. The service provider is responsible for managing the infrastructure for the application software, which avoids the requirement for any upfront expenses for I.T. infrastructure. Because apps are hosted centrally, and upgrades are performed automatically, there is no need for time spent on new installs.

5. DATA LEAKAGE ISSUE IN CLOUD COMPUTING

A cloud can be defined as a vast collection of computers that are connected together over the network. These computers might be private or public and personal or network servers. Let's take the example of Amazon which offers a cloud comprised of both small computers and more considerable large networked computer servers. Amazon's is a private cloud, i.e., Amazon owns it, but that is publicly accessible by the customers on a pay-on-use basis. While the cloud computing concept has been immensely beneficial to many

businesses, it has also presented new hazards. As more firms store information in the cloud, there is a greater risk of sensitive data leaking. Data leakage can be demarcated as an unintended or unplanned transfer of personal or sensitive information to an unsanctioned entity. This might occur if firms are unaware of the need regarding implementation of good cloud security policies. Unsecured storage has resulted in a slew of cloud-related data breaches.

Similarly, cloud misconfiguration is another major cause of cloud-related vulnerabilities that hackers might exploit. When private corporate data including client or patient information, intellectual property and information related to trade secrets are breached, this is referred to as data leakage. When these are disclosed, the company is no longer protected and falls outside of the corporation's jurisdiction. This unregulated data leaking exposes businesses to risk. At the time when the information is not under the private domain, the firm stands in significant jeopardy.

Now the question arises, when is data more vulnerable to getting leaked? Most data get leaked during transit, i.e., when information is transferred from one point to another via wireless or wired connectivity through the internet. The risk of data leakage is very high during transit. Data leakage risk is medium when the data is being used, i.e., a state in which data is currently being utilized, altered, or held in memory of the computer or in the form of cache files at network endpoints. When the information is not being utilized for any reason and is just stored in the any of the storage medium like in a hard disk, in this case the risk of data leakage is medium or low.

In a cloud system, the client is always responsible for assuring security. While cloud service providers have their own rules and practices to ensure safety, organizations' responsibility is to configure the apps. Customers frequently make the typical error of keeping default credentials enabled, resulting in data breaches.

No matter how cautious you are with your personal data, subscribing to the cloud means ceding some control to an outside source. This distance between you and your data's actual location creates a barrier. It may also make it easier for a third party to access your information. However, to get the benefits of the cloud, you are requiring to relinquish direct control over your personal data, but we should not forget that most of the cloud service providers will have extensive expertise in keeping your data secure. A service provider is expected to have greater resources and knowledge as compared to a typical user to safeguard their computers and networks.

6. INCIDENTS OF DATA LEAKAGE

With the ever-expanding cyber world, incidents of data leakage are also becoming very common nowadays. Some of the data leakage incidents are as follows:

6.1. Facebook (2012)

This incident happened in 2012 when it was found in one of the investigations done by KerbsonSecurity. In that investigation, it was discovered that the company was storing the passwords of around 60 crore users in an unencrypted and simple text file format on their servers. But before any kind of mishappening, data was safely secured by Facebook.

6.2. State Bank of India (2018-19)

SBI data leakage occurred from December 2018 to January 2019 when they left one of their servers in Mumbai unprotected, exposing data of around 42.2 crore people. Data leaked contained phone numbers, partial account numbers, and balance details of the customers using State Bank of India Quick service.

6.3. Domino's Pizza (2021)

It happened in February 2021 in which order details of around 18 crores customers were hacked and sold, which was later made available on the Dark Web. This incident happened because the AWS key was compromised due to which details like phone number, name, e-mail address, and location were leaked.

6.4. MobiKwik (2021)

This incident happened on 26th February 2021 and 4th March 2021 when a hacker claimed that he had access to data of around ten crore users, which contains some crucial information like card details and KYC details, and the same was made available on Dark Web for around Rs. 63 Lakh.

6.5. Aditya Birla Fashion and Retail Ltd (2022)

This incident happened on 11th January 2022 when data of around 54 lakh customers and employees was leaked containing e-mail addresses, phone numbers, and passwords. Later, Aditya Birla Group decided to engage some cyber forensic security experts for investigation, and also, they reset the passwords of all the customers and employees.

7. COMPREHENSIVE STUDY OF DATA PROTECTION LAWS IN THE E.U. AND INDIA

7.1. EUROPEAN UNION

To deal with the ever-expanding cyberspace, hike in numbers of data leakage incidents, and safeguard the personal data, European Union in January 2012 decided to come up with a new framework that will be uniformly applied to all countries under E.U.

General Data Protection Regulation was adopted by the European Parliament in April 2016, which was made enforceable in May 2018. GDPR framework demarcates rules regarding collection of data from the people residing in countries under E.U. and processing of that data.

Article 4(7) of the GDPR defines a controller as a decision-making body that takes decision regarding the processing of data. In contrast, when we talk about the processor, it can be referred as a body that deals with the actual process involved in the processing of data and is defined in Article 4(8). The primary difference among the controller and processor is controller will be accountable for complying with the GDPR framework and ensuring that data processing is done with appropriate procedural and legislative measures, whereas the processor has fewer compliance duties.

Article 5 of the GDPR can also be called the entire framework's soul. It contains provisions related to personal data processing principles. To fulfill their obligations, controllers must first comply with these fundamental principles. There are six principles given under Article 5(1), which are as follows:

1. The first principle states that processing of data has to be completed in a transparent, fair way, and for a lawful purpose only. Also, the individuals must be having each and every information related to processing or collection of data.
2. Secondly, the processing of data is to be done for a legitimate purpose only.
3. The third principle states that the processing is to be done only when the objective cannot be achieved by other means.
4. The fourth principle states that the controller has to take every necessary step to verify that the data is accurate and valid for its processing; where he finds that data is inaccurate, he must erase or, if possible, rectify those data on an immediate basis.
5. The fifth principle talks about the storage of data which states that the data should not be stored for any extra time period which is required for processing.
6. The sixth principle provides for the safety and secrecy of the personal data, and the controller has been given the duty to make all the necessary arrangements to confirm that data of the individuals are safe and will never get leaked.

Article 7 states that the controller requires the person's prior consent whose data is subjected to processing, and the matter must be easy to understand if any clause has an ambiguity that makes it against the GDPR. In that case, it will not be binding. Also, individuals are free to withdraw the same at any point of time.

Article 15 provides individuals right to get information regarding their private data, as if their personal data is being processed or processed or whether their data for any reason has been transferred to any third party or any other international organization. These information's can be obtained from the controller.

Under the GDPR, the notion of privacy has been considered as the most crucial aspect. In order to safeguard one's privacy, they incorporated a provision that provides the right to be forgotten. Under Article 17, any individual can approach the controller and ask to erase all the personal data without delay. Also, under Article 21, individuals can object to processing their data when the same is being used for marketing purposes, and the controller has to stop processing.

Article 24 talks about the responsibility of the controller. Article 30 provides that the controller has to record each and every activity concerning the data processing, which shall contain details like the information of

the controller and reasons regarding the processing. In the occurrence of a data leakage, it requires that the Supervisory Authority must be notified by the controller within the period of seventy-two hours, calculating when the controller became aware of the same. Each member nation of the E.U. is free to appoint any number of supervisory Authority as they think fit. The supervisory Authority has been defined under Article 51, which provides that there shall be an independent authority who shall act to protect the people's fundamental rights by monitoring, promoting awareness, and to handle complaints. If required, they can also conduct investigations and act as an enforcement agency under the framework.

In case of infringement, compensation can be claimed by the individuals whose data has been compromised, from the controller or the processor as a matter of right under Article 82 of GDPR for the damages suffered. Also, under Article 83, the supervisory Authority can impose an administrative fine as per the facts and circumstances of the particular case that will be up to twenty million euros or four percent of the total annual turnover worldwide.

7.1.1. Drawback of GDPR

The major drawback of this framework is that it hampers the growth of the companies as they are dependent on the customers, and nowadays, when customers want to have a user-friendly interface, due to this framework, customers have to give endless consents that have increased the burden on customers. Also, corporate firms are facing difficulties complying with this regulation. The compliance cost has also been increased; these things affected the present firms and created a hurdle for the new firms to enter the market. Fines are also one of the primary concerns for businesses.

7.2. INDIA

At present, India does not have any dedicated legislation related to Privacy and the concept of Data Protection. Indian legislation has Section 43A of The Information Technology Act, 2000 (I.T. Act) and The Personal Data Protection Bill, 2019(PDPB).

7.2.1. The I.T. Act, 2000

Section 43A of I.T. Act provides that whenever an enterprise, dealing with or storing personal data of the individuals, fails to keep that data secure, has to pay compensation to the individual whose data has been compromised. But this provision is of no use due to the existence of Section 79, which provides an exception in the case where the body corporate can establish the fact that there was no fault on their side and the leakage that happened is not a part of the transaction initiated them. Hence, in all these cases, it is very easy for the body corporate to establish these facts and make a way out of the scope of Section 43A of the I.T. Act.

7.2.2. Personal Data Protection Bill, 2019

PDPB which is still pending before the parliament, was introduced in the Lok Sabha on 11th December 2019 by then Minister of Electronics and Information Technology, Mr. R. S. Prasad. It was referred to the Standing Committee on the same day, and the committee submitted its report on 16th December 2021.

To understand the Bill, one may require to understand what is meant by data fiduciary, data principal, and data processor, defined under Section 3(13), 3(14), and 3(15) of the PDPB respectively. As per the provisions of Section 3(13), data fiduciary has been defined as a body concerned with making decisions relating processing of data like what needs to be processed, how the processing is to be done, and for what reason the processing is required. The data that needs to be processed is related to a particular natural person, and that person, as per the act, is known as the data principal, and the personal data is defined in Section 3(28) of PDPB. Then comes the data processor, who is actually concerned with the processing that will be done on behalf of the fiduciary.

Section 4 of PDPB provides for the prohibition on the processing; as per the provision in order to do the processing of data, primary requirement of the Bill is that there must be a clear and legitimate purpose for which the processing is to be done. Also, the data fiduciary is required to serve a notice to the individual from whom data is essential to be collected for the purpose of processing, and the notice shall contain details like the purpose regarding the processing and what kind of information is to be collected for that purpose. Under Section 8, data fiduciary has the duty to take care that the data which has been collected from data principal is correct and up to date which is required in the processing. In those case where processing is to be done of data related to a child, in that case, the data fiduciary requires to take consent from his parent or legal guardian after verifying the age of the child.

Every individual, by virtue of Section 17 of PDPB, has a right to get information from the data fiduciary regarding his private data which is processed or being processed, and fiduciary has the duty to provide the same in a simple language which is easily understandable by a lay man. Also, under Section 20, the data principal (individual whose data is concerned) has a right to be forgotten which provides that an individual can approach the data fiduciary and ask to erase all his personal data where the purpose is fulfilled, consent has been withdrawn, or a particular act has been carried out which is against this Bill or any other law.

Privacy is the soul of the Bill, and to ensure privacy of an individual, the fiduciary has duty to manage and do the processing in a way that the privacy of the individual is not compromised and also all steps taken in the process shall be informed to the individual or as per the Bill the data principal. In case of data leakage, the data fiduciary, without any delay, has to report to the Authority with every necessary detail like what kind of data has been compromised, the number of individuals affected, and the consequences and actions taken by them in relation to the leakage occurred.

There shall be an officer appointed under Section 30, and will be known as the data protection officer. The primary responsibility of the data protection officer is to instruct data fiduciaries and monitor the data processing process to ensure that no activities are performed in contravention of the Bill's requirements.

Section 32 of PDPB prohibits the transfer of sensitive personal data (defined under Section 3(36) of the PDPB) outside the territorial jurisdiction of India without the consent of the data principal. Also, regarding

critical personal data, it is restricted to transfer the same for the purpose of processing and any processing thereto has to be carried out within the territorial jurisdiction of India.

There shall be a Data Protection Authority of India, that will be acting as the adjudicatory and enforcement body under the Bill. They shall also be doing functions like monitoring, examination of the reports submitted by the data auditor, promoting awareness, and providing advice to state and central government. Under Section 57, as per the facts and circumstance of the case, the Data Protection Authority may penalize the data fiduciary with the penalty that will be up to rupees 15 Crore or can be even asked to pay 4 percent of the turnover across the nations of the company, and the turnover shall be calculated with respect to preceding financial. Aggrieved by the decision of the Authority, an appeal can be filed under Section 72 of the Bill within 30 days before the Appellate Tribunal, which is established under Section 67. Within 90 days from the decision of the appellate tribunal, one can file an appeal before Supreme Court under the provision of Section 75.

7.2.3. Key Issue with PDPB

One of the primary concerns of the PDPB, is the exemptions given to the government; legislation must review the same and amend the provisions related to exemptions to the government. The Bill was proposed to safeguard the private data of the individuals as the Hon'ble Supreme Court has acknowledged privacy as a fundamental right. Hence, to protect the right of the individuals, the Bill has to be made enforceable on the state and their authorities, but the Bill provides an exemption to the state, which can be held as a violation of fundament rights.

8. SUGGESTIONS

The Personal Data Protection Bill has been enacted in order to ensure the privacy of individuals and protect their data from being misused. To achieve the very objective of the Bill, it is required that the state and state agencies or data fiduciary acting under the state must not be provided with any kind of exemption under the Bill, as an individual has the right to privacy that can be violated by the state itself; hence, the Bill must be amended and exemption must be provided for some specific provisions only. Also, the scope of Section 91 of the PDPB, 2019, is much wider in nature, and in some cases, it would be very difficult to distinguish between personal and non-personal data; hence, proper legislation is required to deal with the concept of non-personal data.

In cases where consent is taken form the parents or the legal guardian of a minor child whose data is concerned; it is required by the data fiduciary must get the consent from the child after he attains the age of majority.

If the data transfer seems to be against the public policy, such data must not be transferred outside the jurisdiction of India even after the consent has already given by the individual whose data is concerned.

There has to be a specific timeframe provided in the Bill for the reporting of data breach incidents. If one goes by the provisions of Section 25 of the PDPB, 2019, it only provides that the reporting has to be done without any delay. A similar provision is there in Article 33 of the GDPR, 2016, which also provides a timeframe of 72 hours.

9. CONCLUSION

In this ever-expanding cyber world, it is necessary to take care of your private data. To keep the private data secure, legislation across the world needs to enforce data protection framework. In order to cope with this issue, countries like E.U., China, Australia, etc., successfully come up with data protection framework. Also, India is able to draft a bill regarding this, but it is pending in the parliament, and also, some considerable changes are required to be made in order to satisfy the need of the society. But when you look at the darker side, you will find that many countries like Pakistan, Afghanistan, Sri Lanka, Nepal, etc., do not have any framework regarding the protection of data. In this present epidemic situation where countries are trying their best to make a way out of the current situation. Every sector depends upon the internet, whether it's for working or academics. A tremendous amount of data is being stored and transferred across the globe, resulting in increased pressure on the digital platform, which may lead to data leakage. Hence, it is required by every nation to enact and enforce the data protection bill without any delay.

10. REFERENCES