Indic Legal Law Journal

ISSN: 2583 - 6385

Volume No. 1
Issue No. 5
December 2022 - January 2023
Pages: 01 - 04
Author Name: Athira R Nair

DATA PROTECTION AND RIGHT TO PRIVACY IN INDIA

ABSTRACT

Lately, the world has made an entrance to the arena of Digital Data Transfer which involves the international exchange of information and has raised the issue of compromised security. In an effort to combat this, India has come up with suitable legislation. The Supreme Court in its Puttaswamy judgment declared the right to safeguard the privacy of individuals as a fundamental right. Following this, the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, introduced the Personal Data Protection Bill in the Lok Sabha in December of 2019. This bill was inspired by the 2018 draft prepared by the now-retired Justice B.N. Srikrishna which had to do with the General Data Protection Regulation. This article aims to briefly analyze data protection and the Right to privacy in India and provide an overview on the pros and cons of the Personal Data Protection Bill of 2019.

INTRODUCTION

The process of safeguarding salient information from falsification or compromise is known as data protection. At times, it is also referred to as data privacy or information privacy. The main aim of data protection is to ensure that the personal details of individuals remain private and are not misused or mishandled. This is a pressing issue in today's world as there are several instances of people facing severe difficulties owing to their private details falling into wrong hands. Ensuring data privacy, quick restoration, and safekeeping are the key components of a data protection strategy. Privacy is one of the most crucial issues while dealing with data protection. Though it's not explicitly provided under the Constitution, privacy indirectly falls under the right to privacy as personal liberty guaranteed by Article 21. It is a multi-dimensional concept that can be construed as a group of rights. In today's digital world, privacy is one of the major contemporary concerns

of the constitutional law seeing that the terms and conditions of almost all the web pages include permission for these pages to intrigue into the user history to know the interests of the user. Furthermore, there are increasing privacy concerns regarding identity theft as this is the wildest and most frequent crime of these days seeing that every 79 seconds, an identity is being stolen. Cases of accounts being hacked and information being leaked are on the rise too. An ingrained dispute between the right to privacy and data protection is evident. The data of individuals and organizations should be protected in such a manner that their privacy rights are not compromised.

In order to combat the existing issues regarding data protection and privacy, the Government of India came up with The Information Technology Act(2000)[1]. This Act was the primary law in India dealing with cybercrime and electronic commerce. In 2008, however, this act was amended in order to address issues the original bill failed to cover and accommodate further development of IT and related security concerns since the original bill was passed. This act The Information Technology (Amendment) Act, 2008[2] deals with both data protection and privacy but in a very vague manner. Since the IT Act is not sufficient in the protection of data, separate legislation in this regard is required. To establish a Data Protection Authority for the protection of personal data of individuals, the Minister of Electronics and Information Technology in India, Mr. Ravi Shankar Prasad proposed the Personal Data Protection Bill 2019[3] in the Parliament on 11th December 2019. This act proposes to protect personal data relating to the identity, characteristics trait, attribute of a natural person along with data deemed sensitive such as that relating to finances, health, identification, sex life, sexual orientation, biometric data, genetic data, caste, tribe, religious beliefs, political inclination, and the like. In addition to this, with the coming of this act organizations would have to follow several compliances while processing personal data in order to ensure the protection of privacy of individuals. Consent of the individual would be necessary for processing personal data, data protection policies would have to be reviewed based on the type of data timely, codes would have to be made consistent with the revised principles, appropriate technical and organizational measures would have to be implemented to prevent misuse of data

[1] The Information Technology Act, 2000. (India)
[2] The Information Technology (Amendment) Act, 2008. (India)
[3] Personal Data Protection Bill,2019.(India)

and grievance redressal mechanisms would have to be appointed to address complaints by individuals. A Joint Parliamentary Committee analyzed the Bill in March 2020 after consulting both experts and stakeholders. However, the reading of the right to privacy into Article 21 of the Indian Constitution by the Supreme Court has become a burning issue due to the concerns raised against the government's initiatives to collect personal data from citizens. Moreover, many people believe that the Act formed by passing such a bill is just an attempt to create a complex legal framework for data protection. As a result of this, both the Right to Privacy and the Data Protection Bill is at stake.

The Personal Data Protection Bill of 2019 aims to protect sensitive data of individuals using personal identifiers like biometrics and financial details. The individuals' data is collected by various data fiduciaries who then handle data processing, which as a matter of fact is how big corporations personalize advertisements and make profits. This bill is made to ensure that the data of individuals is respected and not misused by the government and corporations looking to make profits off of people's personal information. This bill too, like most things, is a double-edged sword with both pros and cons.

Coming to the advantages, advertisements would top the list. India has seen considerable digital evolution in the past two decades. In fact, according to NITI Ayog, today India boasts of 700 million internet users. The downside however would be increased cases of internet fraud and spam which unfortunately led to India being among the top 5 countries affected by cybercrime. In order to combat this, the Personal Data Protection Bill curbs instances of cybercrime by giving individuals more tightened security in the digital world, curbing the spread of fake news, and educating individuals on how to secure their internet data. In addition to this, it also ensures that individuals are entitled to certain rights. Section 7 of this bill aims to increase awareness amongst internet users regarding the nature and purpose of data collection and Section 6 sets the extent of data to be collected by putting a ceiling on it. Apart from this, data localization is being taken up in order to ensure ease of access to data for investigation purposes hence facilitating law enforcement authorities. This will also ensure the government has an increased ability to tax internet bigwigs. Strong data protection also helps enforce data sovereignty. To abide by these newly set up rules, corporations and other bodies who collect data will have to bring about structural and technical changes.

Moving on to the disadvantages of this bill. The first would be the loopholes and lack of a definitive structure. Since the government had legitimate reasons like national security guarding their unchecked access to personal data of citizens, the individuals were prone to have unsolicited government intrusion in their lives thus defeating the very purpose of this bill. Moreover, many believed that despite information being within the state, encryption cannot be ensured by national agencies since the physical location of data is irrelevant in the cyber world. The policy of data localisation didn't sit well with technology giants like Facebook and Google who feared the domino effect this may cause, inconveniencing them once all other countries follow suit. They advocate for a competitive internet market place instead of one with nationalistic borders and stood against the protectionist regime brought into effect by this Bill. In addition to the aforementioned cons, this also acts as a hassle for India's own young startups that are attempting to grow globally.

CONCLUSION

Privacy is a basic human right and computer systems especially in this day and age contain large amounts of data that may be sensitive. Even though data protection may cover a wide area ranging from financial details to health-related sensitive data, the risk of someone accessing information related to anyone from anywhere at any time still poses a threat to private and confidential information. With the coming of globalization, technology has become all the more indispensable to human beings to a level where one couldn’t fathom doing even a simple task like finding directions to a nearby grocery store without it. The researcher is of the opinion that in today’s connected world it is very difficult to prevent information from escaping into the public domain. Data once fed into the web stays there for time immemorial. The right to privacy is recognized in the Constitution but its growth and development are entirely left to the mercy of the judiciary. This one aspect should be changed immediately keeping in mind the risk it poses to a magnitude of the population with a virtual identity. To conclude it would suffice by saying that to counter the problem of protection of data, the emergence of separate, effective legislation is much needed. An effective balance should be struck between personal liberties and privacy in order to achieve the same.