December 2022 (№24)
Volume 8; Issue 4; Page No. 34-40
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/8.4.3

A CRITICAL ANALYSIS OF PERSONAL DATA PROTECTION BILL 2018 WITH REFERENCE TO DATA PROTECTION AND THE RIGHT TO PRIVACY IN INDIA

Sharad Kumar Pandey
Research Scholar, Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Raebareli Road, Lucknow, India

Dr. Pradeep Kumar
Assistant Professor, Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Raebareli Road, Lucknow, India

ARTICLE INFO

Article History:

Received 25.09.2022
Accepted 02.12.2022
Published 28.12.2022

Keywords:

Data Protection Bill, Right to Privacy, Constitutionality, Regulatory Framework

ABSTRACT

Purpose: The purpose of writing this research is to find an analysis of the Data Protection bill with reference to the parameters of data protection and the right to privacy attached to it. The bill contains lot many aspects of creating privacy standards and the legislation related to data protection is much needed for an hour.

Aim: The aim of the study specifically covers the aspects of digital data and its protection related to it. The study covers aspects related to bill wherein the individual data protection considers to be an important part that creates trust between the person and entity/organization handling data.

Methodology: This study is based on a doctrinal approach and analyzes the recent bill and existing laws for the data protection bill. The study specifically represents the recent bill of data protection and existing laws related to data protection and how the statistics show that there is an increase in digital transactions required to share data.

Outcome: The outcome of this paper suggests that the data protection bill incorporates various in the form policies and mechanisms to drive out the personal and individual protection of data. The graphical representation in this study shows that there is a rapid change in technology wherein digitalization is required to keep the legislation related to data protection. Across the world, there are many countries that have a comprehensive regulatory framework wherein the expert committee was set under the Chairmanship of Justice B N Srikrishna to examine to requirements and issues of data protection and its probable solutions.

INTRODUCTION

A new regulatory framework to control the protection of personal data is now being adopted in India. The Committee of Experts, under the direction of Justice B.N. Srikrishna, drafted the draught Personal Data Protection Bill, 2018. We observe that, notably in relation to processing by private entities, the draught Bill provides data subjects with a sizable number of data protection principles and rights. But there are a few crucial areas where the stances taken by the Bill need to be reviewed. This comprises rules governing the composition and layout of the Data Protection Authority, the function of adjudication officers, the flow of data across international borders, and the range of legal exceptions, particularly as they apply to government organizations. In Article 21 of the constitution, the right to privacy is recognized as a derived or implied fundamental right. The court stressed the necessity of enacting strict rules regarding data protection and privacy when it announced its decision on the Privacy Judgement. Indeed, there was a pressing need for such a law to protect the personal information of Indian data subjects because their privacy was in danger due to the crucial role that data played in the development of the digital economy.

KEY SUGGESTIVE AREAS OF THE BILL FOR REVISITING

Firstly, reviewing the regulations controlling cross-border data transfer is necessary, especially in light of their overbroad nature, the minimal privacy improvements it would provide, and the potential repercussions on freedom of speech and other rights. Second, the scope of exemptions granted to government agencies for security and law enforcement purposes needs to be reviewed in order to bring the provisions into compliance with the Supreme Court's decisions in Puttaswamy v. Union of India and ensure an adequate balance between the rights to individual privacy and the needs of state security. Thirdly, it has analyzed the jurisprudential development and current status of the law of privacy in India as well as the numerous model privacy laws that have been created over time. The State was primarily the source of privacy worries in the beginning. Fourthly, aside from the exemptions listed in Chapter IX of the Bill, a number of points need to be reviewed. A more acceptable balancing of privacy with competing rights, such as the freedom of expression and the right to employment, will be achieved through introducing categories like academic and creative activity and nuanced changes to the scope of current exemptions.

MULTI DIMENSIONALITY OF RIGHT TO PRIVACY VIS-À-VIS DATA PROTECTION BILL, 2018

The concept of a person's right to privacy is complex. An individual's special right to manage the gathering, use, and disclosure of his personal information is referred to in the context of personal data. Personal information includes things like a person's name, address, phone number, email address, likes and dislikes, daily routine, family history, education, communication, health, and finances, among other things. We now live in a time where individuals' personal information can be creatively exploited for a variety of reasons, such as government surveillance and commercial revenue generation. The fact that certain methods, such as clustering, geotagging, and geocoding, allow for the unauthorized use of a person's personal data is noteworthy. Other companies may be able to contact the person who shared the photo and give him unwanted adverts, leading to a possible sale. This should highlight the fact that 'data' has the capacity to both empower and hurt, as well as to reveal its salient implications. Innovations in technology have made it possible to communicate and access.

The fact that "data" may empower people as well as cause them damage. Innovative technologies undoubtedly make personal data more accessible and transferable. As a result, it is crucial to create a strong and efficient data protection policy that will strike a balance between innovation and privacy protection. Therefore, resolving all the competing interests in information should be the main goal of a successful data protection law.

PROMINENT FEATURES OF THE BILL

It is better to evaluate the proposed Bill in the context of the European Union General Data Protection Law since the latter has emerged as the initiative leading data protection efforts while the former is still in the executive branch. The research will include two distinct narratives: the anatomical, or exclusive rights, examination of fundamental label and provision; and the skimming orientation of the ruling class. The Committee stressed the importance of striking a balance between privacy and speech when determining whether the right to be forgotten is appropriate. Instead of the right to be forgotten, this matter should have been addressed under "the lawfulness of the processing." When it is determined that the data principal's disclosure of the information is solely personal in nature and unrelated to the public interest, there is a greater balance of expediency for the data theme than for the fiduciary.

CONSTITUTIONALITY ON RIGHT TO PRIVACY IN INDIA VIS-À-VIS SHORTCOMING OF DATA PROTECTION BILL, 2018

The right to privacy is not stated expressly in the Indian Constitution. While taking into account various cases of government interference with personal privacy, Indian courts had taken the argument that the right to privacy is a basic right into consideration. The Personal Data Protection Bill, 2019, is the latest in a long line of privacy laws in India that have been impacted by both national and international trends. A right to privacy exists even though it is not expressly stated in the constitution, according to Indian courts, because Article 21's guarantee of the right to life also includes a right to privacy.[1]

In Kharak Singh v. State of Uttar Pradesh[2], K. Subbarao and K.C. Shah, JJ., delivered a minority/dissenting judgement of the Supreme Court and recognised the right to privacy as a fundamental right protected by Articles 21 and 19(1)(d) of the Indian Constitution. This is another significant ruling worth mentioning. The U.P. Police Regulations' daily surveillance rules were being examined by the Court in this case. Following a dacoity accusation, the petitioner was found not guilty. According to the majority decision in the case, there is no constitutionally protected right to privacy. Two causes that grew more important made it necessary to clarify this ambiguity: (1) vociferous complaints of loss of privacy following the government's adoption of its initiative for unique biometric identity; and (2) concurrent worldwide developments.

Another judgment where the right to privacy will bring out an edging outcome is that in this case[3], CBI requested access to the Unique Identity Authority of India's database in this instance in order to look into a criminal offense. According to a temporary ruling from the Supreme Court, the Unique Identity Authority of India is not allowed to give any other agency any biometric data about a person who has been given an Aadhaar number without that person's express written permission.

The K.S. Puttaswamy v. Union of India[4] case, where the Unique Identity Scheme was considered in relation to the privacy problem, was decided, was significant. Given that there is no explicit privacy provision in the Indian Constitution, the Court was asked if the right to privacy is guaranteed by the Constitution and, if so, what constitutes the source of such right. Privacy is not a fundamental right, according to India's attorney general. In the end, the Court deferred to a bigger Constitutional Bench to consider the issue because past rulings that rejected the right to privacy were rendered by benches larger thn those that determined instances where the right was acknowledged as a fundamental right.

A number of challenges challenging the legality of the legislation enabling the system, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act of 2016, were filed before the Supreme Court as a result of privacy concerns regarding Aadhaar. The five-judge bench of the Supreme Court that examined the petitions stated that it was crucial to first establish if

1 Govind v. State of Madhya Pradesh AIR 1975 SC 1378; R. Rajagopal v. State of Tamil Nadu AIR 1995 SC 264; PUCL v. Union of India AIR 1991 SC 207. State of Maharashtra v. Madhukar Narayan Mardikar AIR 1999 SC 495

2 1964 SCR (1) 332.

3 Unique Identification Authority of India v. Central Bureau of Investigation (2017) 7 SCC 157

4 (2017) 10 SCC 1)

the right to privacy was recognised by the constitution because the petitions alleged infringement of that right. It sent this matter to a bench of nine Supreme Court justices, who then determined that privacy was a part of this right to privacy under Article 21 and that the Supreme Court had erred in its Kharak Singh decision.

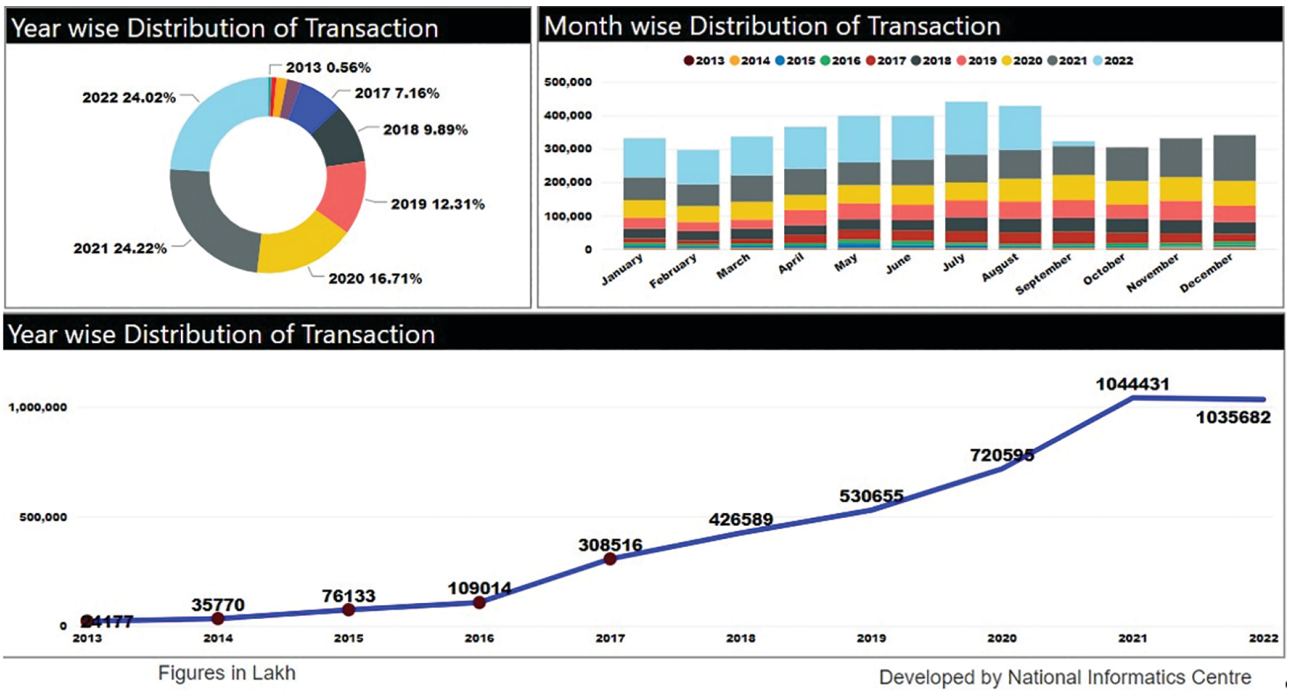
CHALLENGES OF DATA PROTECTION IN AN EPOCH OF BIG DATA

Big data and data are now a new source of enormous economic and social values as well as the basic building blocks of manufacturing. Businesses, governments, and individuals now have access to a much wider range of information thanks to developments in data mining and analytics as well as a dramatic rise in processing power and data storage capacity. Scientists have had to coin new terminology, such as zettabyte and yottabyte, to depict the flood of data due to the rapid growth of the amount of data being generated and stored worldwide. According to Andeson and Raini, when determining whether the right to be forgotten was appropriate, the Committee placed a strong emphasis on striking a balance between the right to privacy and the freedom of speech.

A number of fundamental principles serve as the foundation for international data protection measures like the OECD Guidelines, European Directive, APEC Privacy Framework, and national data protection laws around the world. Restrictions on further use include I ensuring that personal data isn't processed excessively or for purposes other than those for which it was originally collected (generally, personal data cannot be used for other purposes without the consent of the individuals), (ii) providing individuals with information about any personal data processing, and (iii) ensuring that personal data is only used for legitimate purposes.

WHETHER GDPR-STYLE DATA PROTECTION LAW WORK FOR INDIA?

India currently lacks a cross-sectoral data protection law, despite the EU having recognised a right to the protection of personal data for some time (under the Treaty on the Functioning of the European Union). Although it has some rules regarding the protection of personal data, the Information Technology Act of 2000 largely regulates matters like cybercrime and the accountability of internet intermediaries, such as social media plat-



Source: *Representation developed by National Informatics Centre*

forms. For instance, the act's section 43A offers compensation for harms brought on by a failure to uphold appropriate security procedures to safeguard sensitive personal data. But only a hodgepodge of sector-specific legislative standards governs the requirements for data protection and confidentiality.

The EU IA stated that harmonising privacy standards would be one of the primary economic benefits of implementing the GDPR in the EU. It is important to consider what economic advantages the proposed bill would bring to India given that it does not have the issues associated with an outdated, disjointed legislative structure for data protection. The patchwork of existing privacy-related central regulations in India was passed by the federal parliament and is consequently uniform throughout the country. As a result, if one were to analyse the GDPR's three key advantages for the EU in reference to India, at least one of them would not be immediately applicable.

DEVELOPMENT OF PERSONAL DATA PROTECTION IN INDIA

Data can be used for good, but the arbitrary and unchecked use of data, particularly personal data, has sparked worries about an individual's liberty and privacy. This was also the topic of the Supreme Court's historic decision, which recognised the right to privacy as a basic human right. A Committee of Experts has been formed by the Indian government to examine various data protection-related concerns and make recommendations for a draught data protection law. The purpose is to "promote the expansion of the digital economy while maintaining citizen privacy and personal data security and protection.

The distribution of online transactions clearly shows that it is increasing every year and to make it secure a data protection bill is required. The distribution curve clearly shows that the digital transaction significantly increases with time due to which there is a requirement of creating a comprehensive framework. The imminent data protection rule will broaden the scope by providing a thorough data protection outline that shall apply to the dispensation of personal data by any method and to processing activities carried out by both the government and the sequestered entities—not just body corporate-instead of just body corporate.

IMPLICATION OF DATA PROTECTION LAW IN INDIA

Information has become the only resource people rely on in the modern world. With the help of social internet platforms like Facebook, Skype, Whatsapp, and others, society is now interconnected through a single informational thread. These social media platforms have become so important to people nowadays that they are used as a conduit for sharing every last detail of their lives. People from all over the world now communicate with one another on these social media platforms, creating a new dimension of the world. Therefore, through developing effective legislation, it is crucial to secure data from being misused by people or the government.

Social media is a form of Internet-based communication. In addition, there are numerous additional forms of social media, such as blogs, microblogs, wikis, webpages, widgets, and virtual worlds. The popularity of social networking services like Facebook, Twitter, WhatsApp, and others has increased significantly in recent years. To use a social media site, however, and to find other accounts, the person needs first to create a database.

Digitization is a term used to describe the process of creating a numerical sequence that describes a distinct set of an item, image, sound, document, or signal points. The third industrial revolution, known as the digital economy, is a new productivity platform that has emerged globally. It is also known as The Internet Economy or The Internet of Everything (IoE), and it is predicted to create new job prospects, market growth opportunities, and the largest commercial opportunity in human history. It is interesting how quickly our technological advancement has accelerated thanks to Digital India. The goal of the Digital India Program is to make India a hub of global connectivity.

CONCLUSIONS & SUGGESTION

A person's or group's right to privacy refers to their capacity to conceal or separate information about themselves in particular. Although the definition of what is personal and its content differ between cultures and people, they all have some common ground. Privacy is occasionally associated with namelessness, the desire to go unnoticed or anonymous in the public sphere. When something is personal to a person, it typically means that they perceive it as exceptional or delicate in some way. The extent to which private information is revealed in this way will vary depending on how it is gathered in the open, contrasting between locations, and over time.

A protected modification is needed whereby privacy rights can be explicitly guaranteed by adding another agreement, therefore the necessity for a constitutional amendment. A change like that is necessary to provide protection by offering side recognition. In this sense, the law would impose limitations on how individual data customers might gather and utilize personal information. Clients for personal data would be expected to clearly inform the public about the purpose of collecting and using personal data. It is essential to have a thorough confidentiality agreement in place to protect each person's right to exercise resistor over the collection and transmission of their own personal data.

BIBLIOGRAPHY:

1. Kumar, A. (2019). The Right To Be Forgotten in Digital Age: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR. *Shimla Law Review*, *2*.
2. Chowdhury, G. R. (2021). Right to Privacy and Data Protection in India. *Issue 4 Int'l JL Mgmt. & Human.*, *4*, 2602.
3. Singh, S. S. (2011). Privacy And Data Protection In India: A Critical Assessment. *Journal of the Indian Law Institute*, 663-677.
4. Patel, N., & Conners, S. E. (2008). Outsourcing: data security and privacy issues in India. *Issues in Info. Sys. J*, *9*, 14-20.
5. Prasad M, D., & Menon C, S. (2020). The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology*, *28*(1), 1-19.
6. Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.
7. Doneda, D., & Zanatta, R. A. (2022). Personality rights in Brazilian data protection law: a historical perspective. In *Personality and Data Protection Rights on the Internet* (pp. 35-53). Springer, Cham.
8. Determann, L., & Gupta, C. (2019). India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018. *Berkeley J. Int'l L.*, *37*, 481.
9. Riyadi, G. (2021). *Data Privacy in the Indonesian Personal Data Protection Legislation* (No. 7). Policy Brief.
10. Bailey, R., Bhandari, V., Parsheera, S., & Rahman, F. (2018). Comments on the (Draft) Personal Data Protection Bill, 2018. *Available at SSRN 3269735*.
11. Coleman, D. (2018). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Mich. J. Race & L.*, *24*, 417.
12. Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Colum. Bus. L. Rev., 494.
13. Hoel, T., & Chen, W. (2018). Privacy and data protection in learning analytics should be motivated by an educational maxim—towards a proposal. Research and Practice in Technology Enhanced Learning, 13(1), 1-14.
14. Oganesian, T. D. (2020). The right to privacy and data protection in the information age.
15. Bailey, R., Bhandari, V., Parsheera, S., & Rahman, F. (2018). Comments on the (Draft) Personal Data Protection Bill, 2018. Available at SSRN 3269735.
16. Paterson, M., & McDonagh, M. (2018). Data Protection in an era of Big Data: The challenges posed by big personal data. Monash University Law Review, 44(1), 1-31.
17. Park, G. (2019). The changing wind of data privacy law: A comparative study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act. UC Irvine L. Rev., 10, 1455.