SHIELDING YOUR DIGITAL FORTRESS: DATA GOVERNANCE FOR REGULATORY COMPLIANCE AND DATA PROTECTION

Diya Jain*

"Digital freedom stops where that of users begins."

-Stephane Nappo

INTRODUCTION

There has been a considerable increase in the quantity of data generated by various electronic devices and applications over the past couple of years. Today's businesses derive substantial value from 'big data' analysis and frequently base their business strategies on such analysis. There is no refuting of the business efficacy involved, but the burning question is whether or not individuals have control over how their information is accessed and processed by others. It is imperative for individuals, in their capacity as citizens and consumers, to possess the necessary resources to effectively exercise their entitlement to privacy and safeguard their personal information from any kind of misuse or exploitation. This phenomenon is especially evident in relation to our personal information. Data protection pertains to the preservation of our inherent entitlement to privacy, which is firmly established in global and local legislations and agreements. The concept of data protection is frequently characterised as the legal framework established to safeguard individuals' private information, which is acquired, manipulated, and retained using "automated" methods or intended for inclusion in a structured record-keeping system. In contemporary countries, the establishment of data protection laws plays a crucial role in granting individuals the ability to exercise authority over their personal information and safeguarding them from potential misuse. These laws serve to regulate and influence the actions of both corporate entities and governmental bodies. These organisations have consistently demonstrated their tendency to engage in comprehensive data collection, extraction, and retention practises unless regulatory frameworks are in place to limit their actions. Furthermore, they have been seen to adopt a non-transparent approach, providing minimal information to the public.

*BBA LLB, THIRD YEAR, DES SHRI NAVALMAL FIRODIA LAW COLLEGE.

GENESIS/HISTORY

In the year 2017, the Supreme Court held privacy as a Fundamental right of an individual, and the privacy of personal data was an important aspect of the Right to Privacy. Moving ahead in the year 2018, a committee of experts named the 'Sri Krishna Committee', chaired by Justice BN Srikrishna, submitted a draft Personal Data Protection Bill (PDP), and a report to the government titled 'A Free and Fair Digital Economy: Protecting Privacy, 'Empowering Indians'. Next in December. 2019, the PDP Bill was introduced in Lok Sabha, which was a version revised by MeitY that was based on stakeholder consultation and recommendations. Subsequently, in March 2020, a Joint Parliamentary Committee report expected by the Budget Session extended to the second week of the Monsoon Session of Parliament. In September 2020, The Joint Parliamentary Committee examining the Bill gave another extension to submit the report during the Winter Session of Parliament. Further in November 2020, in the Winter Session, the Bill was not tabled and was likely postponed to be tabled during the Budget Session in February 2021. Then in November 2022, Meity released a draft Digital Personal Data Protection Bill for public consultation. Finally, on 5th July 2023, the Union Cabinet approved the draft DPDP bill, 2023

The landmark judgement 2017 Supreme Court decision in K.S. Puttuswamy v. Union of India ("Puttaswamy Judgement") established the need for uniform data protection laws in India by establishing the right to privacy as an element of the right to life and liberty guaranteed by Article 21 of the Indian Constitution. The Supreme Court of India declared that the right to privacy is not an absolute right and any invasion of privacy by the state or non-state entities must fulfil the triple test as follows; Legitimate Aim, Proportionality, and Legality. The 9-judge bench of the Supreme Court held that the judgement that was given in the case of M.P. Sharma v Satish Chandra, which said that the Right to Privacy is not protected by the Constitution, stood overruled. Similarly, the judgement in the case of Kharak Singh, which held that the Right to Privacy is not guaranteed by Part 2, stood overruled. It was finally held that the Right to Privacy of an individual is protected under Article 21 of the Constitution and is also an intrinsic and integral part of the scheme of part 3 that guarantees the fundamental rights of each citizen. Since the Puttaswamy judgement focused mainly on an Individual's rights with that of the state and not on an individual personal life, the Supreme Court ruled that the State had the burden of protecting the dignity of its citizens.

DIGITAL PERSONAL DATA PROTECTION BILL 2023

The Lok Sabha passed the "Digital Personal Data Protection Bill, 2023 on August 3, 2023. On August 9, 2023, the Rajya Sabha passed the DPDP Bill in response.

The DPDP Bill specified that the DATA can be processed or shared by an entity only after acquiring the consent of the concerned individual or entity. It safeguards the rights of an individual by imposing penalties to prevent misuse of sensitive personal data. All of this said data was categorized under three sections such as general, sensitive, and critical. Furthermore, it specifies that the government will have the authority to obtain any user's non-personal data from the companies. The Bill also mandates that all of the critical financial data has to be stored in Bharat; whereas the sensitive data has to be stored in Bharat but can be processed outside with consent only. The DPDP Bill also advised the social media firms to formulate a voluntary verification process for the users. It also levied a penalty of 15 crore rupees or 4% of global turnover if the data is shared without obtaining consent, and data breach or inaction will entail a fine of 5 crore rupees of 2% of the global turnover. The aforementioned legislation bestows upon individuals a multitude of rights with the primary objective of reinstating power to their possession, including the right to information, right to withdraw consent, right to correction and erasure, right of grievance redressal, ensuring transparency and informed consent.

This legal framework also has substantial extraterritorial reach. The Data Protection and Digital Privacy (DPDP) framework imposes extensive obligations, requiring strict adherence to legally justified reasons for processing personal data in a digital format. It also establishes obligations regarding the limitation of purposes for data usage, along with the corresponding duty to delete the data once the intended purpose has been fulfilled. This framework appears to restrict the possibility of utilising personal data for secondary purposes. Additionally, the DPDP framework grants individuals certain rights pertaining to the collection and usage of their personal data, such as the right to be informed, the right to access their data, and the right to have their data erased. The legislation further establishes a regulatory body known as the Data Protection Board of India (Board), which possesses the capacity to conduct investigations into grievances and impose penalties. However, it lacks the jurisdiction to provide guidelines or establish laws.

PENALTIES IN DIGITAL PERSONAL DATA PROTECTION ACT, 2023

According to the DPDP Act of 2023, individuals possess the entitlement to lodge a formal grievance with the Data Protection Board of India (DPB), the designated regulatory authority formed under the aforementioned legislation, in the event of suspected or encountered instances of non-compliance by a third party involved in the collection or processing of personal data. The Data Protection Board (DPB) has the authority to investigate the complaint, prescribe appropriate corrective or mitigation actions, examine relevant documentation, summon and enforce the attendance of any person, and levy fines for non-adherence.

The legislation stipulates that breaches or non-compliance are subject to monetary penalties, which vary from INR 50 crore to INR 250 crore. Notably, a maximum penalty of INR 500 crore is imposed for substantial data breaches. Individuals have the option to pursue reparation from the DPB for any damages incurred as a result of the third party's failure to adhere to regulations. Nevertheless, the legislation does not establish legal responsibility or incarceration as consequences for failure to comply.

JUDICIAL PRONOUNCEMENTS ON RIGHT TO PRIVACY AND DATA PROTECTION LAWS IN INDIA

R. Rajagopal v. State of Tamil Nadu (1994):

This legal case solidified the recognition of the right to privacy as an inherent component of the right to freedom of speech and expression, as outlined in Article 19(1)(a) of the Constitution. The Supreme Court ruled that the dissemination of an individual's personal information without their explicit consent would constitute a breach of their right to privacy.

Selvi and Ors. v. State of Karnataka (2010)[9]: This case dealt with the issue of the admissibility of evidence obtained through narco-analysis and other forms of involuntary testing. The Supreme Court held that such methods of obtaining evidence violate an individual's right to privacy and dignity under Articles 20(3) and 21 of the Constitution.

Justice K. S. Puttaswamy v Union Of India: Under this case, the Aadhar scheme was challenged saying it violates fundamental rights to privacy and equality. He argued that the collection of biometric data by Govt. agencies without any suitable legislation are contravention to privacy. The Supreme Court held that a fundamental right to privacy is guaranteed under the Constitution of India

CONCLUSION

Each path leading to debates on this subject converges at a crossroads known as 'privacy'. The positives and negatives of any single legislation or rule will always be evaluated through the prism of the goals for which they were enacted as well as the impact those goals have on the fundamental rights of each given individual. Considering India's status as one of the major data marketplaces globally, the implementation of a comprehensive data protection and governance policy is expected to have a significant impact on the development of the global data governance landscape. In summary, the Digital Personal Data Protection Bill of 2023 is emerging as a significant legislative measure with wide-ranging implications for several businesses. The implementation of this bill establishes a precedent for the conscientious management of data, enhancing consumer confidence and cultivating a safe digital environment for all stakeholders. As several industries adjust to this emerging paradigm, the shared dedication to safeguarding data establishes the foundation for a prosperous digital economy that prioritizes privacy and security. The DPDP Act represents India's distinct position on contemporary data protection, which has been enhanced by comprehensive post-draft consultations. Although the terms of this legislation are not as comprehensive as those found in regulations such as the General Data Protection Regulation (GDPR), it requires a substantial change in the manner in which Indian enterprises address privacy and personal data.

REFERENCES

(1). **Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.** (2017) 10 SCC 1.

(2). **Information Technology Act, 2000** (No. 21 of 2000), India Code (2023 ed.).

(3). **The Personal Data Protection Bill, 2019,** (Bill No. 373 of 2019)

(4). The Draft Digital Personal Data Protection Bill, 2022, Ministry of Electronics and Information Technology, November 18, 2022.

(5). Ministry of Electronics & IT, "Salient Features of the Digital Personal Data Protection Bill, 2023" (*pib.gov.in*, August 9, 2023) <https://pib.gov.in/PressReleaseIframePage.> accessed October 24, 2023

(6). **Digital Personal Data Protection Act, 2023** (No. 31 of 2023), India Code (2023 ed.).

(7). R. Rajagopal v. State of Tamil Nadu, 1995 AIR 264.

(8). Selvi and Ors. v. State of Karnataka, (2010) 7 SCC 263.