Regulatory measures of Data Protection in India: Need of the hour

[1]Himanshu, [2]Isha Bhardwaj

Final Year Law Student
Law College Dehradun

***Abstract*: This paper deals with the regulatory concerns of data protection in India in the present scenario. The historical background, general development and the issues with the data protection laws in India have been discussed. The authors put forward certain suggestions for the efficient regulation and enforcement of data protection laws, with special reference to the Personal Data Protection Bill, 2018. The need for a specific legislation and a governing body for protection of private data has been stressed. The recent developments in the data protection norms in India were considered with the help of various articles. The paper further emphasizes on the accountability of data handlers. The authors aim to capture key concepts and the potential concerns surrounding data protection norms and try to throw light on the urgent need for the same.**

Index Terms: Data Protection, Need of the Hour, Privacy, Data Protection Bill, 2018.

I. INTRODUCTION

In a recent judgment, Justice D Y Chandrachud wrote, "*Ours is an age of information. Information is knowledge. The old adage that 'knowledge is power' has stark implications for the position of the individual where data is ubiquitous, an all-encompassing presence*."[1]The growth of digitization of economy in India has been a commendable step towards development in the every sector. Through rapid digitalization and agile technology, the concept of "data" has become the new raw material of business, being regarded as an economic input almost on a par with capital and labor.[2]

The government has been demanding access to data from its citizens for the same, which has raised data protection concerns. The Indian laws offer little protection against the misuse of data. Currently, the SPD (Sensitive Personal Data) rules 2011 govern the transfer of personal data and have proved to be inadequate for the task.[3] The Data Protection Bill proposed in 2018 is a step further in the regulatory sphere of data protection. It makes individual consent central to data sharing. It also provides for use of personal data in a fair and reasonable manner and recognizes privacy as a fundamental right. But the concern at this hour is related to the adoption and implementation of the bill.

II. WHAT IS DATA AND DATA PROTECTION?

Data is a wide term which includes both personal aspects of individual and commercial aspects. The personal aspect is dealt under privacy rights whereas the commercial aspect is dealt under proprietary rights. The Information Technology Act, 2000 defines Data under Section 2(1)(o) as- *data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer*.

For the purpose of this research, we will be using the meaning of data as given in The Private Data Protection Bill, 2018- *"Data" means and includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means*.

While we reap its benefits, protection of data is also vital. Protection of Data can be understood in simple terms as a process of safeguarding important information from corruption, compromise, or loss. The importance of data protection has increased with the growing amount of data created and stored. The excessive use has given rise to threat of cyber-crimes, data-theft, misuse of private and personal information etc. A large part of data protection is the adoption of a data protection strategy which should encompass three things- that data can be restored quickly after data corruption or loss, protecting it from compromise, and ensuring data privacy.

[1] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., Writ Petition (Civil) No. 494 of 2012

[2]Kenneth Cukier, "Data, data everywhere", The Ec0n0mist, L0nd0n, February 25, 2010, available at http://www.ec0n0mist.c0m/n0de/15557443.

[3] Radhika Merwin, 'All you wanted to know about Personal Data Protection Bill 2018' in The Hindu

III. EVOLUTION OF DATA PROTECTION LAWS IN INDIA

The digital revolution which is underway in this technology age, has permeated India as well. Recognizing its significance, and that it promises to bring large disruptions in almost all sectors of society, the Government of India has envisaged and implemented the "Digital India" initiative. With nearly 450 million Internet users and a growth rate of 7-8%, India is well on the path to becoming a digital economy, which has a large market for global players.[4]

India has witnessed various instances 0f Data theft as stayed by cyber protection cells. Therefore, to curb data theft, effective and well-formulated mechanism is required. The existing data protection laws in India are narrow in scope. In the absence of specific legislation, data protection was achieved in India by the provisions of The Information Technology Act, 2000, amended by the Information Technology (Amendment) Act, 2008.[5] But, this act is not data or privacy protection legislation per se. It is a generic legislation and does not lay down any specific data protection or privacy principles.[6]

In April 2011, after European Union enacted strict and stringent Data Protection laws, the Indian Ministry of Communications and Technology published four sets of rules implementing certain provisions of the act out of which the first set of rules is relevant to the issue of data protection. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (2011) framed under Section 43A of the IT Act are also a part of this list of legislations. Section 43A states that if 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, this body corporate will become liable to pay damages as compensation to the affected person.

It gives definition of sensitive personal data. It states that *"sensitive personal data includespasswords; financial information, such as bank account or credit card 0r debit card 0r 0ther payment instrument details; physical, physiological and mental health conditions; sexual orientation; medical records and history; biometric information; any details relating to the above clauses as provided to a body corporate for provision of services; and any information received under the above clauses by a body corporate for processing, or which has been stored 0r processed under lawful contract 0r otherwise."*

No legislation provides definition of personal data except IT rules. Further the IT Rules cast a duty upon the Body Corporate to provide a privacy policy which shall be available 0n the website 0f such Body Corporate.[7] The policy shall deal with the personal information and sensitive data including purpose of collection and its usage. The IT Rules m0re0ver deal with the process and procedure that should be adopted by the Body Corporate for collection 0f the personal information and sensitive data.[8] It also states that the Body Corporate cannot retain the information longer than it is lawfully required.[9]Therefore, it can be said that the new law is stricter and stringent and in par with EU laws, the Body Corporate has duty to comply with IT Rules and ensure transparency in its new privacy policies.

However, the existing mechanism however still lacks in the sphere of Protecting the data because the statutes in question were not drafted specifically with the protection of data in mind, the current legislation has a lot of gaps regarding effective protection of data. For this, the government proposed the Privacy Bill in 2011 but the Bill has not become a law yet.

IV. AT THE OUTSET OF THE DATA PROTECTION & REGULATORY CONCERNS

Indian government after considering the fact that the laws were not implemented keeping in mind pers0nal data protection, has proposed to enact specific legislations 0n Privacy. A Data (Privacy and Protection) Bill, 2017 had also been introduced in the parliament by a private member seeking the establishment of a Data Privacy and Protection Authority for regulation and adjudication of privacy-related disputes.

The Data protection may also sometimes occur through The Copyright Act 1957. Since it protects intellectual property rights in different types of creative works including literary works, it provides some scope for protecting different types of data as literary works. Moreover, The Indian Penal Code 1860 could be used to prevent theft of data.

In all India does not have a large data protection and regulation framework. A strict regulation covering all aspects of data protection and encompassing provisions of all the scattered legislations needs to be adopted to protect private data. With growing threat to privacy from both the State and non-State elements, the government should "put into place a robust regime for data protection".[10]Further, there maybe multiple rules and regulations that directly 0r indirectly govern privacy and data protection

[4] https://meity.gov.in/; Last visited 01.05.2019.

[5] The Information Technology Act, 2000.

[6] Mohammed Nyamathulla Khan, 'Does India have a Data Protection Law?' in Legal Service India.

[7] Rule 4 0f IT Rules

[8] Rule 5 0f IT Rules

[9] Rule 5(4) 0f IT Rules

[10] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., Writ Petition (Civil) No. 494 of 2012

domain in India, which include the IT Act, Right to Information Act, Right to privacy, Aadhaar Act and rules framed thereunder and additional regulations governing sectors such as telecom, banking, medicine and healthcare and insurance.

V. WHETHER EXISTING MECHANISM IS ADEQUATE?

After a critical analysis of the literature, the authors attempt to bring to light the lacuna in the proper adoption and implementation of the laws made for protection of private data. The need for a specific legislation cannot be denied. But we need to ask more questions. Questions related to accessibility concerns. By whom and to what extent is personal data being accessed? Accountability question, the question of the establishment of a data protection authority, the question of adjudication of cases related to data breach and other regulatory concerns. The paper shall further deal with a discussion on the said issues with special reference to The Personal Data Protection Bill, 2018.

VI. THE PERSONAL DATA PROTECTION BILL, 2018

The Personal Data Protection Bill, 2018 is India's move to provide its citizens with comprehensive data protection rights. It was drafted by a committee headed by former Supreme Court judge Justice B N Srikrishna on July 27th, 2018. It forms the framework for India's data protection laws and explains how an organization should collect, process and store citizens' data. The objective of Personal Data Protection, 2018 is to "ensure growth of the digital economy while keeping personal data of citizens secure and protected."

The Applicability 0f the bill is on both government and private entities. The applicability of the law will extend to data controllers / fiduciaries or data processors not present within the territory 0f India, if they carry 0ut processing of personal data in connection with any business carried in India, systematic 0ffering 0f good and services to data principals in India 0r any activity which involves profiling 0f data principals within the territory 0f India. Further, the bill entrusts data principals with stronger control over informati0n about them. All in all it will definitely change the way privacy is perceived and practised within Indian paradigm.

It states right to privacy as a fundamental right and necessitates protection of personal data as an essential facet of informational privacy. One of the most important proposals in the committee's white paper was that a high-powered statutory authority with regulatory capacities should be set up. It also mentions two models, the European Union's, tilted towards privacy of individuals and the US, giving innovation primacy over regulation, and says that India will have to follow a nuanced approach towards data protection.[11] The bill aims to protect personal data and has a wide applicability. It states that personal data can only be processed on the basis of the following:

- Consent of the owner;
- If being used for the function of the state;
- If mandated by law or required for compliance of a judicial order;
- If necessary for an emergency;
- For employment purposes;
- For reasonable purposes as notified by the data protection authority.

At the outset, the bill provides excessive powers in the hands of the central government, especially under Section 98 which not only states that the central government can issue directions to the authority, but also that the authority shall be bound by directions on questions of policy in which the decision of the central government is final.[12] Moreover, the criminal liabilities making all offenses cognizable and non-bailable under this bill are worrying.

VII. IMPACT & CHALLENGES 0F THE PROPOSED BILL

Data protection has been a hot topic for discussion among businesses, academia, interest groups and think tanks. The bill is under review and speculation and a topic for debate as to its means and end. Debates and journals have tried to cover almost all its aspects and brought to light what is not and what should be. The authors will also throw light on what should be stressed- what is the need of the hour.

It is criticized for being too lenient and lacking in clarity on key issues. However, with the bill coming into force, the 0rganizati0ns will have t0 ensure that they handle the personal data judiciously. The requirements for notice, consent and grounds 0f processing personal and sensitive personal data will force organizations to redesign their core systems, 0btain fresh consent, and change their data practices that will eventually increase the cost 0f compliance for companies. Though the draft bill addresses

[11]Krishn Kaushik, 'What India needs: Data law, regulator' in The Indian Express

[12]Ananya Bhattacharya, "India's first data protection bill is riddled with problems" in Quartz India

various escalating issues 0f the personal data ecosystem in India and clearly articulates the rights of individuals, yet it falls short 0n key landmines that form the center 0f a robust data protection framework.

VIII. NEED OF THE HOUR

It is clear from the above discussion that the fundamental need is of a specific legislation in the area which should cover all aspects of data protection- the what, the how and the by whom. What is the data that is to be protected? Is mere protection of private data enough? What about commercial data and business data? What all authorities does India need to set up in order to ensure efficient regulation of the protection of data? These are only some of the many concerns that data protection raises.

The Private Data Protection Bill 2018 does have certain lacunas but is a step in the right direction and should be carried forward to be made an act after its speculation. An independent dedicated Data Protection Authority having a specialized structure should be set up and be given reasonable powers as may be necessary for an efficient adjudication and dispersal of data privacy issues. It should have sufficient jurisdiction and power to adjudicate disputes and issue binding orders. It could be quasi-legislative body to prescribe rules and procedures. It could include people from the know-how, experts, and persons of adequate qualification, backed by police intelligence authorities- local and central, so that speedy remedy can be given. Also, it must have a judicial wing.

Moreover, in terms of transparency and accountability, data controllers and processors should adopt certain measures based on standards and regulations having fixed liability in case of data breach. There should be implementation of data protection principles and if required, demonstration of such implementation by a supervisory authority in order to ensure greater accountability. Also, a system should be in place to detect and prevent data breach. As data breach involves issues of privacy, which is a fundamental right under Article 21 of the Indian Constitution,[13] it becomes necessary to take measures against it.

IX. CONCLUSION

Data protection law in India is currently facing many problems due the absence of proper legislative framework.[14]But with the enactment of the Personal Data Protection Bill 2018, we will have an overarching regulation that will be more effective and overshadow all existing privacy laws. The ongoing explosion of cybercrimes, and theft and sale of stolen data has raised issues and concerns worldwide. India, with much of its population having an online identity, could easily fall victim to cases of cybercrimes and, data and privacy breach.

Absence of data protection law is also a huge blow to the outsourcing industry in India. By creating a good data protection law, India could extend well beyond being a mere supplier of services to the world's multinational corporations. Whatever steps the government can take right now in the wake of the hour, it should and the rest shall follow. The process is slow but is achievable if taken seriously by the authorities. The Private Data Protection Bill 2018 is a right start to a needful end. Justice Srikrishna has most appropriately noted in regard to the bill, '*The report is like buying new shoes. It's tight in the beginning but it will become comfortable over a period of time. It remains to be seen if the citizens of India get used to these shoes or return them.*'

[13] The Constitution of India.

[14] Mohammed Nyamathulla Khan, 'Does India have a Data Protection Law?' in Legal Service India