

BURNISHED LAW JOURNAL

PERSONAL DATA PROTECTION BILL, 2019 AND THE ROLE OF STATE

Archit Majumdar

One cannot see the impact or implementation of legislation while at the same time ignoring the role of State and how the legislation has been drafted. While regulation by the State is extremely necessary to base, to not give complete autonomy to bodies, it is important to see that the State does not compromise and negatively impact the implementation. The Personal Data Protection Bill, 2019 is certainly a step taken for the proper codification of data protection laws, but the question remains whether the degree of the role of State towards the implementation of the same, is justified or not. From the front, the Data Protection Bill is necessary as highlighted in the B.N.Srikrishna Committee which has been cited as the foundation of the Data Protection Bill. The B.N. Srikrishna Committee had highlighted the importance of data localization to be revolving around the lines of efficiency of enforcement, reduced reliability on fiber optic cables, growth of an AI system and dissolving foreign surveillance¹. But the question remains on the impartiality and the independence of the Authority formed under the legislation.

The primary objective of the act is the privacy of the data subjects and data protection works under that. One prime element under data protection now, is the Right to be Forgotten. Section 20 of the Personal Data Protection Bill, 2019 talks about the Right to be Forgotten. Right to be Forgotten is fundamentally a step taken in the light of privacy measures where the subjects can have their existence erased from the accounts of the Data Processor as well as Data Fiduciary. Section 20 of the Bill says that the data principal shall have the right to restrict or prevent the continuing disclosure of his data by a data fiduciary under 3 scenarios when i) the purpose of collection of the data has been fulfilled, ii) when the collection had been initiated by consent of the principal and the consent has now been withdrawn, iii) collection is being made contrary to the Act or any law

¹Committee of Experts under Chairmanship of B.N.Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics and Information Technology Jan 20, 2020, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

in place². But this erasure of the data from the data processor and data fiduciary can be made after appealing to the Adjudicating Officer appointed under Section 62 of the Bill. This Officer will decide on it based on the scale of availability, the relevance of the data, the role of the data principal to determine whether the erasure can be made. On turning down of the appeal, the principal can appeal again, but this appeal will still go to the Adjudicating Officer. The problem here is that the Adjudicating Officer is appointed by the Data Protection Authority under Section 62 of the Bill. The Data Protection Authority is in turn appointed by the Central Government under Section 41 of the Bill and the Chairperson and the member would be chosen by a committee consisting of the Cabinet Secretary, the Secretary to the Government of India in the Ministry or Department dealing with the legal affairs, the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information and Technology. Therefore, the entire appointment of the Data Protection Authority and the Adjudicating Officer are directly and indirectly influenced by the Government. Hence, the right to be Forgotten which is fundamentally an extension of the Right to Privacy, is dependent on the authorities put in place by the Government.

The B.N.Srikrishna Committee report, the base document on which the Bill has been formulated had noted that a dysfunctional protection law could potentially compromise domestic surveillance, give rise to censorship³. It also noted the importance of a body for external checks on the data protection body. But the Data Protection Bill, 2019 does the contrary to what the Committee suggested. The Bill, which is arguably stricter than the General Data Protection Regulation, concentrates significant power on the State and thus, compromises the implementation of the Bill. The Bill gives power to the Government to access personal data on the grounds of security of the State, the sovereignty of the State, foreign relations and public order. None of the grounds has been defined in the Bill notwithstanding that the composition of the Data Protection Authority is determined by a Committee composed of State authorities. The State could access any personal data if it deems so because of how vaguely the Bill has been written. Section 35 of the Bill says that the Government if is satisfied on the grounds of sovereignty, the security of the State, foreign relations or public order may deem the Act to do not apply to Government agencies. Furthermore,

² Personal Data Protection Bill, 2019, Bill No. 373 of 2019.

³ Committee of Experts under Chairmanship of B.N.Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics and Information Technology, Jan 20, 2020, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

Section 44 gives the power to the Central Government to remove the Chairperson and members of the Data Protection Authority. Section 68 says that the manner of appointment, term of office, salaries, resignation and removal will be prescribed by the Central Government, and Section 70 says that the officers and employees shall be provided to the Appellate Tribunal by the Central Government. The entire system is dependent on who the Central Government appoints and the chances of the influence of Central Government on the working of Data Protection Authority and thus on personal and non-personal data are significant and cannot be dismissed.

In a paper written by Center for Internet and Society titled 'The Localization Gambit' multiple stakeholders had said that the Act would result in the concentration of powers within the State and thus would result in third party abuse⁴. Professor Graham Greenleaf had highlighted that the statutory authority was lacking in independence and that the regulations were authoritarian⁵. It is important to note that there are no checks and balances whatsoever in the functioning of the Data Protection Authority and leaving it to the exceptions given in the Bill, might significantly put the security of the data in danger.

It is also important to note a key observation of Michael Dell as he put that the Bill could lead to greater digitization, it has potential for abuse. Now it needs to be questioned what is more important, abuse of data or digitization⁶? The big companies will find it better to have this Act in place as this would necessarily eliminate smaller companies from coming into place as it imposes a high cost of functioning, therefore, why not have such an Act at the cost of abuse? Some big companies such as Alibaba had already established data centres before the Bill came into place. The cost of setting up of data centres cannot be met by most data processors and the penalties of not adhering to the Act are significantly high, and hence innovation is also compromised.

Therefore, what is the solution? While in all probability, this Act will pass as it is, there is a need to understand what positive changes could be brought. First of all, exceptions need to be discussed. The constituents of 'public order', security and sovereignty of the State need to be laid down, to

⁴ Arindrajit Basu, Elonnai Hickok, Aditya Singh Chawla, The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India, Center for Internet and Society, Jan 21, 2020, <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>.

⁵ Graham Greenleaf, GDPR-Lite and Requiring Strengthening – Submission on the Draft Personal Data Protection Bill to the Ministry of Electronics and Information Technology (India), Jan 21, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3252286.

create strict grounds on which government can actually in practice get access to the data and not otherwise. The powers of the State have to be limited for better functioning of the Act. Furthermore, the implementation of the Right to be Forgotten has to be re-considered. It should be the individual's choice to determine whether they want their existence to be there or not, and if not, there should be an independent appellate body to determine the appeals to the Adjudicating Officer. There needs to be an independent body which is free from the influence of the State in any form whatsoever, which determines the exercise of the power of the State about the Data Protection Authority. For example, the importance of the separation of the judiciary and executive could be put into place here. Hypothetically, a Committee consisting of former judges of the Supreme Court, members of non-profit research organizations, academicians could be formed to determine whether any action by the State or any access to data on grounds of public order, security and sovereignty of State is valid or not. But certainly, a step has to be taken to avert the risk of total government influence on the Data Protection law as B.N. Srikrishna, the head of the Committee on which the Data Protection Bill has been formulated himself has said about the Bill that, the Bill could potentially turn the country into an "Orwellian State"⁷.

The logo of Burnished Law Journal is a stylized orange emblem with intricate patterns, resembling a traditional Indian motif. It is centered on the page, partially overlaid by the text of the article.

BURNISHED LAW JOURNAL

⁷ Megha Mandavia, Personal Data Protection Bill can turn India into 'Orwellian State': Justice BN Srikrishna, Economic Times, Jan 21, 2020, <https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?from=mdr>.