Exemptions for the State

The Personal Data Protection Bill 2019 (bill),[1] empowers the government to issue an executive order to exempt any government agency from the applicability of the bill. This is applicable when processing of data is necessary for- protecting sovereignty and integrity; security of the state, maintaining friendly relations with foreign states, public order or for preventing incitement to commit cognizable offences.[2] Additionally, compliance with select provisions of the bill has also been exempted, in the cases of investigation, prevention, detection, investigation and prosecution of offences or any other contravention, legal proceedings, domestic purposes and journalistic purposes.[3]

Shortcomings of these Provisions

No legal test: In the *Puttaswamy* Judgment-I[4], the Supreme Court ruled that privacy is not an absolute right, and could be overridden in cases where public interest is more important than individual's interest. In this regard, it empowers the central government to gain access to personal data, subject to satisfying a three-prong legal test of:

1) Legitimacy, to ensure that there is a legitimate aim that necessitates such action by the government;

2) Proportionality, to ensure that action taken by the government is not disproportionate to the aim it is intended to achieve;

3) Legality, to ensure that the abrogation of the fundamental right to privacy should be in accordance with a law.

However, as opposed to the draft bill of 2018[5], this test has been removed from the bill. It empowers the government to completely exempt any of its agencies from the provisions of the bill, while processing personal data for the purposes mentioned under S. 35. Such exemptions based on a mere executive order, are ultra viers of the *Puttaswamy* judgment II[6], wherein the Supreme Court

explicitly stated that executive notifications to be insufficient for restricting the fundamental right to privacy. Enabling unaccounted access to personal data to the government without any mechanism for legal checks and balances will not only increase likelihood of privacy violation by the government, but also fuel risks of surveillance, thereby threatening free speech.

No Limitation on Time: Bill does not specify any limitation on the time for which such data can be retained in case of collection for exercise of exemptions. This could increase the chances of data being stored and used by government agencies or data processors beyond the purposes of collection of data in such cases, putting privacy of data principal at considerable risk.[7]

Broad Exemptions: There is a departure in the bill from Draft Bill of 2018[8], which gave exemptions with respect to only certain provisions of the bill such as purpose limitation, collection limitation, consent but still made an exception to ensure fairness and reasonableness in processing and security safeguards. This is specifically relevant to section 35, which gives a broad mandate to government in exempting governmental agencies from the applicability of the entire Bill.

Recommendations

Reinstating the Legal Test: The three-prong legal test must be reinstated along with specifying that such exemption could only be applied through procedure established by law, for both section 35 and section 36. This legal test is essential to prescribe appropriate substantial and procedural safeguards to maintain the reasonableness and fairness in applying restriction to the fundamental rights.[9] This will also ensure the constitutionality, transparency and accountability by government and its agencies. Additionally, the government should prescribe clear guidelines and provide for appropriate judicial order, instead of mandating the exercise of exemption just on the basis of an executive order. We should adopt from the best practices of European Union's (EU) General Data Protection Regulation (GDPR)[10] and Asia-Pacific Economic Cooperation (APEC) privacy framework[11], which also provide for safeguards of necessity, proportionality and as prescribed by the law along with maintaining transparency through public disclosure.

Ensuring Purpose Limitation: The bill should ensure that data is only used with respect to the purpose of exemption, 'purpose limitation' in exercise of exemptions must also be specified. This could be done through stipulating that usage of data must be limited to the purposes of exemptions and that data

should only be retained only until the time such purpose is completed and must be deleted thereafter. In this regard, APEC privacy framework also specifies limitations for use only for the objectives of exemptions.12 Further, the bill should require for the government to conduct a cost benefit analysis to assess if benefits outweigh the cost of exercising exemptions.

Narrowing Exemptions: The bill should limit the scope of exemptions within section 35 by providing the agencies to adhere to provisions relating to notification of breach, offences, penalties, data audits and security safeguards. These are important provisions which protect rights of data principals in cases of misuse of data and helps ensuring transparency.

---

1   The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

2   S. 35 of the bill.

3   S. 36 of the bill.

4   Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others SC WP(C) No. 494 of 2012

5   Clause 42 of the Draft Bill of 2018

6   Justice K.S.Puttaswamy (Retd) vs Union of India, (2019) 1 SCC 1

7   Justice B.N Srikrishna Committee Report, 2018

8   Clause 42 (2) of the Draft Bill of 2018 "Any processing authorised by a law referred to in sub-section (1) shall be exempted from the following provisions of the Act— (a) Chapter II, except section 4; (b) Chapter III; (c) Chapter IV; (d) Chapter V; (e) Chapter VI; (f) Chapter VII, except section 31; and (g) Chapter VIII."

9   Justice K S Puttaswamy (Retd.) and Another Vs. Union of India and Others SC WP(C) No. 494 of 2012

10   Article 23(1) of the GDPR

11   Part ii (13) APEC Privacy Framework

12   Part ii (13) APEC Privacy Framework