Data Protection Bill: The provisions and the reasons for rolling it back

August 16, 2022

Manifest Pedagogy:

The government has withdrawn the Personal Data Protection Bill from Parliament as it considers a "comprehensive legal framework" to regulate the online space, including bringing separate laws on data privacy, the overall Internet ecosystem, cybersecurity, telecom regulations, and harnessing non-personal data to boost innovation in the country.In today's digital era, where data security and privacy are constantly under threat, it has become important to save people's private and personal data from being misused. Need of the hour is a robust Data protection bill that will aid in protecting individuals' privacy rights and the fair and transparent use of data for innovation and growth, thus unlocking the digital economy.

In News: Govt withdraws Data Protection Bill, 2021, will present new legislation in coming times.

Placing it in Syllabus: Polity and Governance.

Static Dimensions

- Provisions of the bill
- Journey of the draft Bill

Current Dimensions

- More on news
- Reasons for rolling back the bill
- Need for such a law
- Concerns with the bill

Content

More on news

- The government has taken this step after nearly four years of the Bill being in the works.
- It had gone through multiple iterations, including a review by a Joint Committee of Parliament (JCP), and faced major pushback from a range of stakeholders including big tech companies such as Facebook and Google, and privacy and civil society activists.
- The tech companies had, in particular, questioned a proposed provision in the Bill called data localisation, under which it would have been mandatory for companies to store a copy of certain sensitive personal data within India, and the export of undefined "critical" personal data from the country would be prohibited.
- The activists had criticised, in particular, a provision that allowed the central government and its agencies blanket exemptions from adhering to any and all provisions of the Bill.
- It has been close to 10 years since the (Justice) A P Shah Committee report on privacy, five years since the Puttaswamy judgement (right to privacy) and four years since the (Justice B N) Srikrishna Committee's report they all signal urgency for a data protection law and surveillance reforms. Each day that is lost causes more injury and harm."

Need for such a law

- For the first time, a Bill was enacted to protect the digital rights and privacy of Indians. Global attempts include the **General Data Protection Regulation** implemented by the European Union, and the State data privacy laws in the United States.
    - Even **Brazil** has implemented data privacy legislation.

- While India has some laws to regulate sensitive data under the Information and Technology Act of 2000, no legislation has been passed so far to implement the ethos of the Puttaswamy judgement, which guaranteed Indians their right to privacy.
- As Indians increasingly onboard onto digital platforms, there is an urgent need to protect citizens' personal data and make the data utilisation process transparent.
    - **Around 18 of every 100 Indians** have been affected by data breaches since 2004, with **962.7 million data points being leaked**, primarily personal data points such as names and phone numbers.

Journey of the draft Bill

- The **Justice Srikrishna panel** was set up in 2017 in the backdrop of the Supreme Court's verdict holding privacy is a fundamental right, and its direction to the government to draw up a data protection framework for the country.
    - The Srikrishna Committee released a white paper that same year, outlining the areas it would be looking at.
- In July 2018, the committee submitted a draft data protection Bill to the Ministry of Electronics and IT, which said that it would draft a fresh Bill borrowing from the ideas presented in the Srikrishna Committee Bill.
- In December 2019, the Bill was referred to the JCP. As the committee started a clause-by-clause analysis of the Bill, it also sought and received extensions for presenting its report in September 2020 and March 2021.
- In December 2021, the JCP tabled its report in Parliament, which Justice Srikrishna said was heavily in favour of the government. In a media interview, he said that the Bill could turn India into an "Orwellian state".

Provisions of the bill

- **Applicability:** The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India.
- Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual.
- The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator.
- **Obligations of data fiduciary:** A data fiduciary is an entity or individual who decides the means and purpose of processing personal data.
- Such processing will be subject to certain purpose, collection and storage limitations. For instance, personal data can be processed only for specific, clear and lawful purposes.
- Additionally, all data fiduciaries must undertake certain transparency and accountability measures such as: (i) implementing security safeguards (such as data encryption and preventing misuse of data), and (ii) instituting grievance redressal mechanisms to address complaints of individuals.
- They must also institute mechanisms for age verification and parental consent when processing sensitive personal data of children.
- **Rights of the individual:** The Bill sets out certain rights of the individual (or data principal). These

include the right to: (i) obtain confirmation from the fiduciary on whether their personal data has been processed, (ii) seek correction of inaccurate, incomplete, or out-of-date personal data, (iii) have personal data transferred to any other data fiduciary in certain circumstances, and (iv) restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.

- **Grounds for processing personal data:** The Bill allows processing of data by fiduciaries only if consent is provided by the individual.
- However, in certain circumstances, personal data can be processed without consent.
- These include: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency.
- **Social media intermediaries:** The Bill defines these to include intermediaries which enable online interaction between users and allow for sharing of information.
- All such intermediaries which have users above a notified threshold, and whose actions can impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.
- **Data Protection Authority:** The Bill sets up a Data Protection Authority which may: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Bill.
- It will consist of a chairperson and six members, with at least 10 years' expertise in the field of data protection and information technology. Orders of the Authority can be appealed to an Appellate Tribunal.

- Appeals from the Tribunal will go to the Supreme Court.
- **Transfer of data outside India:** Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions.
- However, such sensitive personal data should continue to be stored in India. Certain personal data notified as critical personal data by the government can only be processed in India.
- **Exemptions:** The central government can exempt any of its agencies from the provisions of the Act: (i) in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and (ii) for preventing incitement to commission of any cognisable offence (i.e. arrest without warrant) relating to the above matters.
- Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as: (i) prevention, investigation, or prosecution of any offence, or (ii) personal, domestic, or (iii) journalistic purposes.
- However, such processing must be for a specific, clear and lawful purpose, with certain security safeguards.
- **Offences:** Offences under the Bill include: (i) processing or transferring personal data in violation of the Bill, punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, and (ii) failure to conduct a data audit, punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher.
- Re-identification and processing of de-identified personal data without consent is punishable with imprisonment of up to three years, or fine, or both.

- **Sharing of non-personal data with government:** The central government may direct data fiduciaries to provide it with any: (i) non-personal data and (ii) anonymised personal data (where it is not possible to identify data principal) for better targeting of services.
- **Amendments to other laws:** The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data.

Reasons for rolling back the bill

- **Dealays**-The delays in the Bill had been criticised by several stakeholders, who had pointed out that it was a matter of grave concern that India, one of the world's largest Internet markets, did not have a basic framework to protect people's privacy.
- **JCP amendments**-The Personal Data Protection Bill, 2019 was deliberated in great detail by the Joint Committee of Parliament. 81 amendments were proposed and 12 recommendations were made towards a comprehensive legal framework on the digital ecosystem.
- Considering the report of the JCP, a comprehensive legal framework is being worked upon. Hence, in the circumstances, it is proposed to withdraw 'The Personal Data Protection Bill, 2019' and present a new Bill that fits into the comprehensive legal framework."
- **Compliance intensive**-The Bill was also seen as being too "compliance intensive" by startups of the country.
    - According to government sources, the revamped Bill will be much easier to comply with, especially for startups.
- **Opposition from stakeholders**-The bill had faced major push back from a range of stakeholders including big tech companies such as Facebook and Google, and privacy and civil society activists.

- **Key discussions of Committee**

- The key discussions in the panel were based on whether the proposed Data Protection Authority should get constitutional status and whether States should have their own Data Protection Authorities.
- The Opposition members had alleged that the penalty provisions on fiduciaries if they breach or process data in an unauthorised manner were watered down despite their objections.
- The JCP's report also recommended changes on issues such as regulation of social media companies, and on using only "trusted hardware" in smartphones, etc.
- It proposed that social media companies that do not act as intermediaries should be treated as content publishers, making them liable for the content they host.

Concerns with the bill

- **Issues with Sections 35 and 12**: Under Section 35, the Centre can exempt any agency of the government from the application of all provisions of the Act; when it is deemed to be in national and public interest.
    - Similarly, Section 12(a)(i) creates the space to exempt the government from provisions of consent, allowing it to collect personal data without individual approval. These blanket exemptions are a cause of concern.
- **Data localisation:** The bill makes a concerted push towards data localisation. But whether or not it will be implemented in a graded manner, depending on the sensitivity of data, is unclear.
- **Surveillance framework:** The bill does not have provisions for the creation of an oversight mechanism.
    - The Data Protection Authority had been entrusted with a wide variety of functions, ranging from standard-setting to adjudication. This will end up

"overburdening" the architecture.

- **Data Protection Authority:** Enforcement of penalties and compensation orders of the DPA does not require a court order
    - The Bill does not specify that a court order would be required for the enforcement actions.

Way Forward

- It is imperative that the Government soon introduces a fresh data protection legislation, covering both personal and non-personal data, drawn after proper public consultation.
- The legislature should acknowledge the significance of data as an asset.
    - Consequently, the provisions regulating non-personal data in the Bill should be directed towards striking a balance between economic development and data protection, in alignment with internationally accepted regulatory design concerning non-personal data.
- Providing individuals with proper grievance redress options and creating sufficient deterrence among private actors.
- Non-personal data has mainly a business dimension and is commercially critical for firms.
    - With India's internet economy taking off, the government should not club personal data and non-personal data
    - India must promote Data Localisation with care and by more scientific and organic categorisations.
- The Committee recommended that individuals have to be alerted to a data breach of any entity collecting their data. But it has to be automatic and unconditional to help victims take precautions such as changing passwords.
- Data captured by electronic hardware should clarify

whether the data include data generated by a company’s internal functions or not.

Mould your thoughts

1. Data protection bill has been recently rolled back by the government. Discuss the need for such a law and reasons behind the roll back. Also suggest measures to make data protection comprehensive in India. (250 words)

Approach to the answer.

- Introduction about data protection law.
- Need for such a law.
- Reasons behind the roll back.
- Suggestions for future law.
- Way Forward and Conclusion.