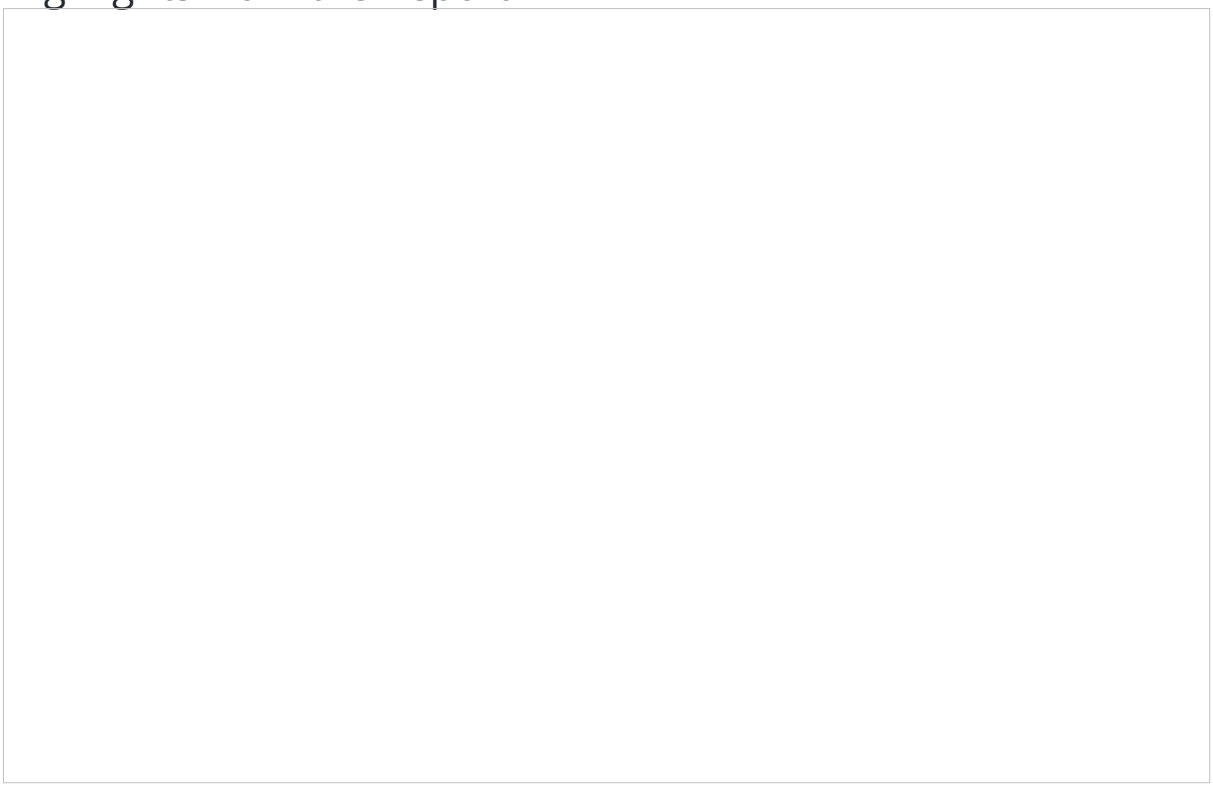
Justice BN Srikrishna Committee Submits Data Protection Report

A committee headed by retired Supreme Court Judge Justice BN Srikrishna has submitted its report on "Data Protection Framework" to the Government.

- The Committee was constituted by the union government in July 2017, to deliberate on a data protection framework.
- The Supreme Court in its **Puttaswamy judgment, 2017** declared privacy a fundamental right. This set the government in motion to take steps to bring a new data protection legislation for the country.
- The report has emphasized that interests of the citizens and the responsibilities of the state have to be protected, but not at the cost of trade and industry.
  The Committee has also proposed a draft Personal Data Protection Bill.

Highlights from the Report



- **Individual Consent:** The proposed Bill makes individual consent the centrepiece of data sharing, awards rights to users, imposes obligations on data fiduciaries (all those entities, including the State, which determine purpose and means of data processing).
    - Consent will be a lawful basis for processing of personal data. However, the law will adopt a modified consent framework thereby making the data fiduciary liable for harms caused to the data principal.
    - The Data Protection Bill also calls for privacy by design on part of data processors, and defines terms like consent, data breach, sensitive data, etc.
    - **Right to be forgotten:** It refers to the ability of individuals to limit, delink, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic.
- **Data Protection Authority:** The data protection law will set up a Data Protection Authority (DPA), which will be an independent regulatory body responsible for the enforcement and effective implementation of the law. The DPA shall perform the following primary functions:
    - monitoring and enforcement
    - legal affairs, policy and standard setting
    - research and awareness
    - inquiry, grievance handling and adjudication

- **Personal Data**: The law will cover processing of personal data by both public and private entities.The law will have jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India.
    - The Bill has proposed that critical personal data of Indian citizens be processed in centres located within the country.
    - Sensitive personal data will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law.
    - Additionally, personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals not present in India.
- **Data Storage:** The Bill lays out provisions on data storage, making it mandatory for a copy of personal data to be stored in India.
- **Appellate Tribunal:**The Central Government shall establish an appellate tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA.
- **Penalties:** Penalties may be imposed for violations of the data protection law. The penalties imposed would be an amount up to the fixed upper limit or a percentage of the total worldwide turnover of the preceding financial year, whichever is higher.
    - The Committee has suggested a penalty of Rs. 15 crore or 4% of the total worldwide turnover of any data collection/processing entity, for violating provisions. Failure to take prompt action on a data security breach can attract up to Rs. 5 crore or 2% of turnover as a penalty.
    - The penalties paid by violating entities in this case will be deposited to a **Data Protection Fund**, which will, among other purposes, finance the functioning of the Data Protection Authority.

- **Obligations on Fiduciaries and rights to principles** are the two underlying themes of the Bill.
    - Obligations would include “purpose limitation” where data will be used only for clear, specific and lawful purposes and “collection limitation” where only data necessary for the purpose would be collected and be held as long as reasonably necessary for the purpose.
    - The Bill lays out obligations for fiduciaries to ensure no harm to the user, with transparency and security safeguards; a data protection impact assessment is embarked upon before new technologies are introduced; data policies are audited by a data auditor; and they have data protection officers.
    - For data processors not present in India, the Act will apply to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India.
- The law **will not have retrospective application** and it will come into force in a structured and phased manner.
- **Impact on allied laws:**The report has also listed the impact of the proposed data protection framework on allied laws, including the Aadhaar Act and the RTI Act, which require or authorise processing for personal data for different objectives.
    - The committee has noted that the Aadhaar Act is silent on the powers of the Unique Identification Authority of India (UIDAI) to take enforcement action against errant companies in its ecosystem. The Aadhaar Act needs to be amended to bolster data protection.
    - The report has also recommended amendments to the RTI Act, pointing out that disclosure of information from public authorities may lead to private harm being caused.
- **Exceptions:** The state can process data without consent of the user on ground of public welfare, law and order, emergency situations where the individual is incapable of providing consent, employment, and reasonable purpose.
    - Processing of data for certain interests such as security of the State, legal proceedings, research and journalistic purpose, may be exempt from certain obligations of the proposed data protection law.
    - However, adequate security safeguards must be incorporated in the law to guard against potential misuse.
- **Cross border data transfers** of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee.

        Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data).

- **Data of Children:** Committee has made specific mention of the need for separate and more stringent norms for protecting the data of children, recommending that companies be barred from certain types of data processing such as behavioural monitoring, tracking, targeted advertising and any other type of processing which is not in the best interest of the child.
    - The justification for such differential treatment arises from the recognition that children are unable to fully understand the consequences of their actions. This is only exacerbated in the digital world where data collection and processing is largely opaque and mired in complex consent forms.
    - The committee's recommends that the Data Protection Authority will have the power to designate websites or online services that process large volumes of personal data of children as guardian data fiduciaries.
    - The committee noted that this approach, of placing the onus of properly processing the data of a child on the company, is preferable to the existing regulatory approach which is based solely on a system of parental consent.
    - The parental concern is prone to circumvention. It risks encouraging children to lie about their age, without achieving the intended purpose of protection.

Concerns

- Though the draft bill addresses various issues plaguing the data ecosystem in India, it falls short on key principles that are at the core of a robust data protection framework
- The Bill proposes that personal data of individuals can be processed for the exercise of any function of the state. This can be done without the consent of the individual as long as it is to provide a service or benefit to the individual. This runs directly counter to the articulation of informed consent as central to informational privacy in the Puttaswamy judgment, 2017.
- One key subject missing from the draft bill is the reform of surveillance laws. There is very little legislative and judicial oversight on surveillance activities carried out in India. As proposed by the Bill, requiring all businesses to store data within India, without any reform of surveillance governance, can pose even bigger privacy issues in the future.

Way Forward

- Bringing in a legislation on the data protection in the country would protect individual privacy, ensure autonomy, allow data flows for a growing data ecosystem.
- It can create a free and fair digital economy where freedom is the enhancement of individual autonomy with regard to personal data and fairness is the regulatory framework where this individual right is respected.