AGENDA 2 : REVIEWING THE JUSTICE SHRI KRISHNA COMMITTEE RECOMMENDATIONS ON DATA PROTECTION AND THE IMPLICATIONS OF THE PROPOSED DATA PROTECTION BILL

Note from the EB:
Esteemed members of Parliament,

As far as data protection goes its breaches and violations can cause a huge threat to national security and its adverse effects can wreak havoc with a stable environment.
Protecting the judicial system has never been more important with the increasing rate of extrajudicial executions and it's systematic victimisation of innocent civilians.

The LOK SABHA brings one of the most challenging agendas which can only be tackled with technicality and precision.

The EB would like to inform you that we would proceed with the amendment of the data protection bill on the premise that it is already been passed as an Act of parliament.

We request the representatives of the Indian people to be thorough and technical with their research .
Good luck, may you succeed in bringing prosperity to our great nation!

Introduction:
India's first step to provide its citizens with comprehensive data protection rights may need more than a few tweaks before it can be considered effective.

On the 27th of July, the justice BN Srikrishna committee submitted the draft Personal Data Protection bill, 2018 to the Union legislature. This bill will form the building blocks for India's data protection laws, deciding how organisations should collect, process, and store data.
In no time after releasing the bill, it was subject to heavy criticism for being too lenient and lacking in clarity on key issues, which in turn resulted in a farrago of ambiguities.

The bill aims at making consent as the primary grounds for data processing. For children, parental consent and use of age verification mechanisms by data fiduciaries would be required. A major shortcoming here however is the exemptions made for the state.

After receiving much criticism the Bill introduced new definitions of personal data and sensitive personal data. Personal data refers to any data on a natural person which allows direct or indirect

identifiability. Sensitive personal data (SPD) also contains religious and political beliefs, caste, intersex/transgender status and official government identifiers.
Financial data as SPD(supra) has also been included, which has been defined to specifically include data like financial status and credit history. Biometric data as SPD also now specifically includes facial images or photographs, but only when processed so as to allow unique identification of the person (such as facial recognition techniques).The Bill will not apply to anonymous or non-personal data.

"Every data fiduciary (any organisation processing personal data, like the ISP's) shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies."

This would imply that companies would have to spend huge amounts on setting up local servers, among other things. This may become a big hurdle for existing companies to operate in India, and new ones to set shop.
"Mandating localisation of all personal data as proposed in the bill is likely to become a trade barrier in the key markets," IT industry body Nasscom said in an email statement. "Startups from India that are going global may not be able to leverage global cloud platforms and will face similar barriers as they expand in new markets."

"The central government shall, by notification, establish for the purposes of this Act, an authority to be called the Data Protection Authority of India…with power, subject to the provisions of this Act, to acquire, hold, and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued."

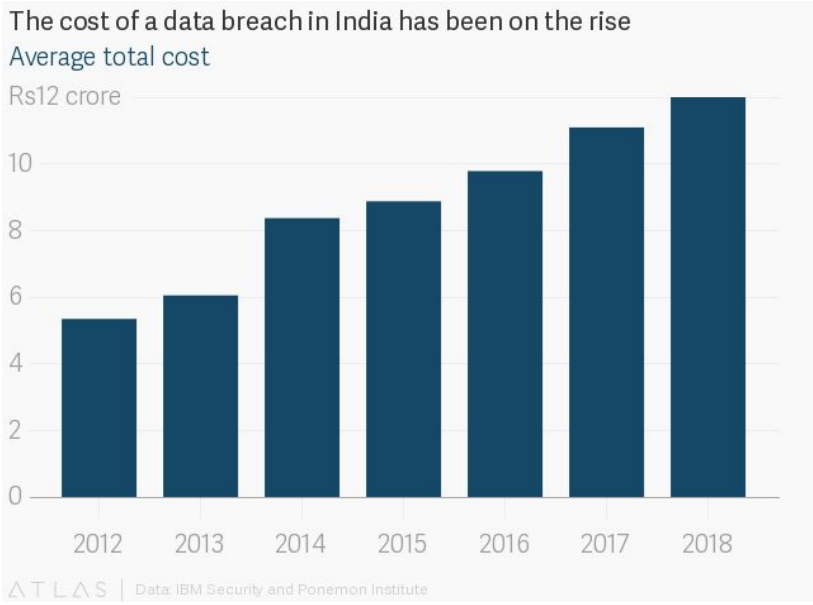
"The data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal (user)."

Although the intention was to improve transparency and accountability, this authority—comprising a chairperson and six other members appointed by the central government would hardly operate autonomously.

Mounting concerns over the privacy of the citizens and the fact that the country is moving towards digital governance, a stringent data protection law is in urgent need. Looming uncertainty over questions that need explanation for ownership of data, custodian of data etc needed to be answered. Rising case of privacy breaches and data harvesting called for the setting up a regulator or adjugation mechanism to deal with the same.

India being part of the the stage for digital economy, digital governance and digital storage of all knowledge, leaves behind large digital footprints. Addressing the issue became the need of the hour.

According to a study conducted by IBM Security and Ponemon Institute, an American research firm data breaches now blow a million-dollar hole in India Inc's pocket.The study covered nearly 500 global companies that experienced such theft. It analysed the cost of stolen records, customer defections, and opportunity loss.
The number of incidents of data theft and cyber attacks has also increased rapidly in the country. Between April 2017 and January 2018, over 22,000 Indian websites, including 114 government portals, were hacked, according to government data. One such incident was reported in May when the personal data of millions of Indians registered with the Employees' Provident Fund Organisation was allegedly leaked.
Indian companies are struggling to cope with such risks. They are taking a lot longer to identify and contain these data breaches, according to the IBM study.
In 2017, the mean time to identify a data breach increased to 188 days in the country from 170 days in 2016. The time taken to contain them, too, has increased from 72 to 78 days, the study says.[1]



1 <https://qz.com/india/1325647/data-breaches-cost-indian-companies-millions-of-dollars-says-ibm-study/. >

EXISTING DATA PROTECTION LAWS

1. EU GDPR

The general data protection regulator, standardizes the data protection laws in all 28 EU countries and imposes strict new rules on controlling and processing personally identifiable information (PII). It also extends the protection of personal data and data protection rights by giving control back to EU residents.[2]

There are eight principles of good information handling outlined in the act that state that data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

2. The United States

The US has no single federal law that covers protection of data, but is an aggregation that can sometimes overlap, dovetail and contradict one another. Some of the most prominent federal privacy laws include, without limitation, the following:

1. The Federal Trade Commission Act
2. The Financial Services Modernization Act
3. The Health Insurance Portability and Accountability Act
4. The Fair Credit Reporting Act (15 U.S.C. §1681)
5. The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
6. The Electronic Communications Privacy Act

3.Australian Privacy Act

[2]https://www.forbes.com/sites/2018/02/14/what-is-general-data-protection-regulation/#5265d5a762dd

The Privacy Act, 1988 regulates how personal information is handled. The Privacy Act includes Australian Privacy Principles (APPs)[3]:

- right for individuals to access and correct their personal information
- the open and transparent management of personal information including having a privacy policy
- an individual having the option of transacting anonymously or using a pseudonym where practicable
- the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection
- how personal information can be used and disclosed (including overseas)
- maintaining the quality of personal information
- keeping personal information secure

Data Protection , AADHAAR and UIDAI:

The Srikrishna Committee was constituted during the pendency of the hearings in the constitutional challenges to the validity of the UID project. The Union government had in fact stated during its submissions to the Supreme Court that it was setting up a committee and intended to introduce laws related to data protection and privacy. Those following the Aadhaar project have waited to see the kind of impact a data protection bill might have on the project, with many feeling that any data protection bill would by its very nature, have to deal with, and curtail it. The idea of a privacy/data protection law has been proposed various times in the country's recent past. None of the various official drafts and deliberations have occurred in a time quite like this, when over one billion Indian

[3] https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

citizens were, in most cases, coerced into enrolling in a centralised mandatory biometric identification system[45].

Regardless of the landmark Judgement on Constitutional Validity of AADHAAR and its findings, the matter is now res-judicata and further discussion pertaining to the issue shall be discouraged.

QARMA:

- Amending the provision pertaining to carte blanche given to the state to process personal data without obtaining consent under section 13.
- Reformation of surveillance laws
- Means to maintain transparency and regular updation of data
- Conditions clearly defining situations in which data may be withheld or disclosed (explicitly mentioning for overseas transfer, under which cases legal protection may or may not be provided)
- Scope, accountability and liability of DPA's to be clearly defined
- Management of consent for disabled and mentally unsound citizens

[4] www.thequint.com
[5] www.thewire.com