Srikrishna Committee - White Paper on Data Protection Framework

Why in news?

\n\n

Srikrishna Committee recently released a white paper as part of its mandate to draft a data protection and privacy Bill.

\n\n

What is the need?

\n\n

\n
- The Committee was set up by the Ministry of Electronics and IT following the decision to make Aadhaar compulsory for many government services.
\n
- Private entities are also increasingly using Aadhaar for the purpose of authentication and financial transactions.
\n
- Notably, the Aadhaar is being issued by the UIDAI after collecting individual's personal and biometric data.
\n
- Despite an obligation to adopt adequate security safeguards, no database is 100 per cent secure.
\n
- Evidently, despite UIDAI's various in-built data protection mechanisms, it is not bound to inform an individual in cases of misuse or theft of his or her data.
\n
- Thus, the interplay between any proposed data protection framework and the existing Aadhaar framework will have to be analysed.
\n

\n\n

What are the highlights?

\n\n

\n
- The committee has identified seven key principles for the data protection law, which include:
\n

\n\n

\n
1. **Technology agnosticism** - flexibility of the law for adapting to changing technologies and standards of compliance.
\n
2. **Holistic application** - governing both private sector entities and the government; differential obligations for certain legitimate state aims.
\n
3. **Informed consent** - informed and meaningful consent of the individual must be ensured by the law.
\n
4. **Data minimization** - Data that is processed ought to be minimal, only for targeted and other compatible purposes.
\n
5. **Controller accountability** - The data controller shall be held accountable for any processing of data.
\n
6. **Structured enforcement** - There should be a high-powered statutory authority with sufficient capacity and decentralized mechanisms for enforcement of the data protection framework.
\n
7. **Deterrent penalties** - Penalties on wrongful processing of data must be adequate to ensure deterrence.
\n

\n\n

\n
- **SPDI** - The white paper has laid down for the protection of sensitive personal data or information (SPDI) by which a person is identifiable.
\n
- This essentially means that any social media site, search engine, telecom operator or government agency cannot sell or disclose SPDI of individuals.
\n
- It has identified health and genetic information, religious beliefs and affiliation, sexual orientation, and racial and ethnic origin as SPDI.
\n
- It has also placed caste and financial information in this category.
\n
- The committee prescribes punishments in case of violations of regulations in

using SPDI.
\n
- At present, the IT Act rules on security practices and sensitive personal data are applicable only to private or corporate entities.
\n
- **Data Breaches** - The law may require that individuals be notified of data breaches where there is a likelihood of privacy harms.
\n
- However the paper noted that fixing too short a time period for individual notifications might be too onerous on smaller organisations.
\n
- As, such an organisation may not have the necessary information about the breach and its likely consequences.
\n
- Thus it is suggested that both government and the private entities be brought under the ambit of the proposed law.
\n
- **Exemptions** - The Committee has made certain exemptions in relation to collecting information.
\n
- This is in reference to investigating a crime, apprehension or prosecution of offenders, and maintaining national security and public order.
\n
- But, the committee also insists on devising an effective review mechanism.
\n
- **Penalty** - A civil penalty of a specific amount may be imposed on the data controller for each day of violation.
\n
- **Besides**, it suggested setting up a data protection authority, data audit, registration of data collectors, enacting provisions for protecting children's personal data, etc.
\n

\n\n

\n\n

Source: Business Standard, LiveLaw

\n