Concerns in the Draft Data Protection Bill

Why in news?

\n\n

The Justice Srikrishna Committee report accompanying the draft Personal Data Protection Bill has been released recently.

\n\n

What are the findings of the report?

\n\n

\n
- The report notes that eight of the top 10 most accessed websites in India are owned by U.S. entities.
\n
- This reality has often hindered Indian law enforcement agencies when investigating routine crimes or crimes with a cyber-element.
\n
- Police officials are forced to rely on a long and arduous bilateral process with the U.S. government to obtain electronic evidence from U.S. communication providers.
\n

\n\n

What are the concerns with the report?

\n\n

\n
- **Data Localization -** The Bill calls for a copy of user data to be mandatorily localised in India.
\n
- It is believed that this will “boost” law enforcement efforts to access data necessary for investigation and prosecution of crimes.
\n
- The draft bill mandates local storage of data relating to Indian citizens only.
\n
- If passed in his form, however, the law will be counterproductive, hurting law enforcement efforts and undermining user rights in the process.

\n
- **Outdated Law -** The bill relies on an outdated Mutual Legal Assistance Treaty (MLAT) process to obtain data stored by U.S.
\n
- By this, technology companies are allowed to share data such as content of an email or message only upon receiving a federal warrant from U.S. authorities.
\n
- This scenario will not change even after technology companies relocate Indian data to India.
\n
- Even if Indian authorities force compliance from U.S. companies, it will only solve a part of the problem.
\n
- **Lack of reforms -** The Bill recognises principles of legality, "necessity and proportionality" for data processing in the interest of national security and investigation of crimes.
\n
- However, it fails to put in place the procedural rules necessary for actualising these principles.
\n
- Even rudimentary requirements such as a time limit for which data can be stored by law enforcement are missing in the Bill.
\n

\n\n

What is the way forward?

\n\n

\n
- Localisation can provide data only for crimes that have been committed in India, where both the perpetrator and victim are situated in India.
\n
- For investigations into such crimes, Indian law enforcement will have to continue relying on cooperative models like the MLAT process.
\n
- The Clarifying Lawful Overseas Use of Data (CLOUD) Act, passed by the U.S., seeks to de-monopolise control over data from U.S. authorities.
\n
- The CLOUD Act creates a potential mechanism through with countries such as India can request data.
\n
- This applies not just for crimes committed within their borders but also for transnational crimes involving their state interests.

\n
- The draft Bill comes as an opportunity to update India’s data protection regime to qualify for the CLOUD Act.
\n

\n\n

\n\n

Source: The Hindu

\n