Data Protection for Minors

This editorial is based on **"Needed, a new approach to data protection for minors"** which was published in The Hindu on 24/01/2023. It talks about the issues with the draft Digital Personal Data Protection (DPDP) Bill, 2022 with respect to children.

For Prelims: Eighth schedule of the Indian Constitution, Draft Digital Personal Data Protection (DPDP) Bill, 2022, Commissions for Protection of Child Rights Act, 2005, the Right of Children to Free and Compulsory Education Act, 2009, and the Protection of Children from Sexual Offences Act, 2012.

For Mains: Draft Digital Personal Data Protection (DPDP) Bill, 2022 and related issues, Data Protection for Minors and its need

The need for data protection for **minors in India is crucial as the country continues to see an increase in the use of technology** and the internet among children. As more and more children access the internet and use digital devices, they are at risk of being exposed to various forms of online abuse, such as cyberbullying, grooming, and exploitation.

The **Draft Digital Personal Data Protection (DPDP) Bill, 2022** is a proposed legislation that aims to protect the personal data of individuals in India. Currently, it **provides for mandatory parental consent for all data processing activities** by children, defined as any person aged under 18 years.

In addition, the **collection and use of personal data of minors without proper consent can also lead to privacy violations** and potential harm. It is therefore **important for India to implement robust data protection measures** to safeguard the rights and well-being of its young citizens.

What are the Major Provisions of the DPDP Bill, 2022?

- **Data Principal and Data Fiduciary:**
  - Data Principal refers to the individual whose data is being collected.
    - In the case of **children (<18 years), their parents/lawful guardians will be considered their "Data Principals".**
  - A Data Fiduciary is the entity (individual, company, firm, state etc), which decides the "purpose and means of the processing of an individual's personal data".
- **Rights of Individuals:**
  - **Access to Information:**
    - The bill ensures that **individuals should be able to "access basic information"** in languages specified in the **eighth schedule of the Indian Constitution.**
  - **Right to Consent:**
    - **Individuals need to give consent before their data is processed** and "every

individual should know what items of personal data a Data Fiduciary wants to collect and the purpose of such collection and further processing".
        - Individuals also have the right to withdraw consent from a Data Fiduciary.
    - **Right to Erase:**
        - Data principals will have the right to demand the erasure and correction of data collected by the data fiduciary.
    - **Right to Nominate:**
        - Data principals will also have the right to nominate an individual who will exercise these rights in the event of their death or incapacity.
- **Data Protection Board:**
    - The Bill also **proposes to set up a Data Protection Board** to ensure compliance with the Bill.
    - In case of an unsatisfactory response from the Data Fiduciary, the consumers can file a complaint to the Data Protection Board.
- **Cross-border Data Transfer:**
    - The bill allows for cross-border storage and transfer of data to "certain notified countries and territories" provided they have a suitable data security landscape, and the Government can access data of Indians from there.
- **Financial Penalties:**
    - **For Data Fiduciary:**
        - The bill proposes to **impose significant penalties on businesses that undergo data breaches or fail to notify users** when breaches happen.
        - The penalties will be imposed ranging from Rs. 50 crores to Rs. 500 crores.
    - **For Data Principal:**
        - If a user submits false documents while signing up for an online service, or files frivolous grievance complaints, the user could be fined up to Rs 10,000.

What are the Issues with Bill with regard to Children?

- **Relies on Parents to Grant Consent:**
    - Instead of incentivising online platforms to proactively build safer and better services for minors, the **Bill relies on parents to grant consent on behalf of the child in all cases.**
    - In a country with low digital literacy**, where parents in fact often rely on their children** (who are digital natives) to help them navigate the Internet, **this is an ineffective approach to keep children safe online.**
- **Does not Consider Children Interests:**
    - It disregards the **"best interests of the child" standard**, which originated in the **1989 Convention on the Rights of the Child.**
        - India has upheld this standard in laws such as the **Commissions for Protection of Child Rights Act, 2005,** the **Right of Children to Free and Compulsory Education Act, 2009**, and the **Protection of Children from Sexual Offences Act, 2012.**
        - However, it has not been applied to the issue of data protection.
    - The **Bill does not factor in how teenagers use various Internet platforms** for self-expression and personal development and how central it is to the experience of adolescents these days.
- **Risk Personal Data of Citizens:**
    - In the current draft of the DPDP Bill, **each platform will have to obtain 'verifiable parental consent' in the case of minors.** If this provision is enforced strictly, it can change the nature of the Internet as we know it.
    - Since it is **not possible to tell if the user is a minor without confirming their age, platforms will have to verify the age of every user.**
        - The **government will prescribe later whether verifiability will be based on ID-proof**, or facial recognition, or reference-based verification, or some other means.
    - Now, all platforms will have to **manage significantly more personal data than before**, and citizens will be at greater risk of harm such as data breaches, identity thefts, etc.

What should be the Way Forward?

- **Designing Services that Protect Children from Harm:**
  - The need of the hour is to **move from a blanket ban on tracking, monitoring, etc. and adopt a risk-based approach** to platform obligations.
  - Platforms should be **mandated to undertake a risk assessment for minors** and not only perform age-verification-related corresponding obligations but also design services with default settings and features that protect children from harm.
    - This **approach will bring in an element of co-regulation**, by creating incentives for platforms to design better products for children.
- **Relaxing the Age of Mandatory Parental Consent:**
  - It is **needed to relax the age of mandatory parental consent for all services to 13 years in line with many other jurisdictions** around the world.
  - **By relaxing consent requirements, data collection will be minimised**, which is one of the principles that the Bill is built on.
  - This relaxation in age of consent in tandem with the risk mitigation approach elucidated above **will achieve protection for children online while allowing them access.**
- **Conducting Large-Scale Surveys:**
  - To tailor this solution to the Indian context, the **government should also conduct large-scale surveys of both children and parents** to find out more about their online habits, digital literacy, preferences and attitudes.
  - A policy should be designed that **balances the safety and the agency of children online.**
  - The onus of keeping young safe **should not be put only on parents,** but instead it **should make it a society-wide obligation.**
- **Improving Children's Right to Privacy:**
  - **Children should be educated about their rights to privacy** and how to protect their personal information online.
  - **Children have a fundamental right to privacy**, and this includes protection of their personal data.
  - However, as technology continues to advance and more information is collected and shared online, it becomes increasingly important to ensure that this right is upheld for minors.
    - The **digital space can have many benefits to children's development** particularly for exploring creativity and self-expression.

Drishti Mains Question

Discuss what measures should be taken to ensure data protection for minors in the digital age?

UPSC Civil Services Examination Previous Year Question (PYQ)

Prelims

Q. Which of the following adopted a law on data protection and privacy for its citizens known as 'General Data Protection Regulation' in April, 2016 and started implementation of it from 25th May, 2018? (2019)

(a) Australia
(b) Canada
(c) The European Union
(d) The United States of America

Ans: (c)

- With objective to impose a uniform data security law on all EU members, General Data Protection

Regulation (GDPR) was approved by the European Union (EU) in April 2016.

- GDPR standardizes data protection law across all 28 EU countries and imposes new rules on controlling and processing personally identifiable information.
- It also extends the protection of personal data and data protection rights by giving control back to EU residents. GDPR replaces the 1995 EU Data Protection Directive, and came into force on May 25, 2018. **Therefore, option (c) is the correct answer.**

Mains

Q. Data security has assumed significant importance in the digitized world due to rising cyber crimes. The Justice B.N. Srikrishna Committee Report addresses issues related to data security. What, in your view, are the strengths and weaknesses of the Report relating to protection of personal data in cyberspace? **(2018)**