PERSONALITY TEST PROGRAMME 2019
(Current Affairs Interview Issues)

THE PERSONAL DATA PROTECTION BILL, 2019

Introduction

Data is any collection of information that is stored in a way so computers can easily read them (011010101010 format). It usually refers to information about our social media messages and posts, online habits, online transactions, medical records, other personal details etc.

Companies, governments, and political parties find this data valuable because they can use it to find the most convincing ways to advertise or shape our opinions online. For example- The Facebook–Cambridge Analytica data scandal of 2018 where personal data of millions of peoples’ Facebook profiles without their consent was used for political advertising purposes.

About Data Protection

- **Data protection** is the process of protecting the personal data and aims to strike a balance between individual privacy rights while still allowing data to be used for myriad purposes.
- Several countries have dedicated law for data protection like Japan’s Act on Protection of Personal Information. European Union has also adopted General Data Protection Regulation 2018.
- **India does not have any dedicated legal framework for data protection.** Presently some acts cover the data protection in general.
  - Sec 43A of Information Technology Act 2000 protects user data from misuse but it is applicable to only corporate entities and not on government agency. Also, the rules are restricted to sensitive personal data only — medical history, biometric information among other things.
  - Other acts like Consumer Protection Act 2015, Copyrights Act 1957 among others also attempt to protect the personal information.
- In 2018, a draft version of the bill was prepared by a committee headed by retired Justice B N Srikrishna.
- Recently, the **Personal Data Protection Bill, 2019** was introduced in Lok Sabha by the Minister of Electronics and Information Technology.

Need of Data protection

- **Invasion of privacy:** India has around 40 crore internet users and 25 crore social media users who spend significant time online. Extremely personal aspects can be shared with different stakeholders without someone’s consent.
  - Without effective data protection there could be increased surveillance, profiling of individuals etc.
  - For e.g. Recently, 121 Indian citizens’ WhatsApp accounts were hacked by an Israeli software called Pegasus.
  - Supreme Court in K.S. Puttaswamy case has declared Right to Privacy is a Fundamental right. Hence protecting individual privacy is constitutional duty of the state.
- **Economic losses:** According to Cost of a Data Breach report per capita cost per lost or stolen record reached Rs 5,019 in 2018, which represents an increase of 9.76 per cent from the prior year.
  - Moreover, data is considered as new oil in 21st century. Without any proper data regulations or data localisation norms, we are virtually giving away this asset to foreign companies. Generally, applications...
About Right to be Forgotten (RTF)

It refers to the ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or outdated.

EU’s GDPR states that individual shall have the right to obtain from the controller the erasure (deletion) of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data.

At present, the right to be forgotten is not well-established in India.

Unlike the GDPR, the Personal Data Protection Bill, 2018 only provides for prevention of continuing disclosure of personal data and not the deletion of personal data.

The grounds for exercising this right include cases where the disclosure of the personal data has served the purpose for which it was made or is no longer necessary; this determination has to first be made by an Adjudicating Officer.

The Adjudicating Officer also has to be satisfied that the right to be forgotten overrides the right to freedom of speech and expression, and the right to information of any citizen.

Challenges/ constraints in data protection

- India does not have capability for data localization i.e. to store data within country.
  - Most of the data storage companies are based abroad. They also export data to other jurisdiction making it difficult to apply Indian laws.
- There hundreds of private players are involved in data dynamics which makes it difficult to apply uniform data protection framework.
- It is usually difficult to trace the perpetrator invading the data privacy.

About the Personal Data Protection Bill, 2019

It seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. Its specific provisions are:

- Personal data (data that can identify an individual): The bill talks about various types of personal data, such as:
  - Sensitive personal data (related to finances, health, official identifiers, sex life, sexual orientation, biometric, genetics, transgender status, intersex status, caste or tribe, religious or political belief or affiliation)
  - Critical personal data (military or national security data and the government can define it from time to time)
  - General personal data- other than sensitive and critical personal data.
- Applicability: The Bill governs the processing of personal data by:
  - Government
  - companies incorporated in India
  - foreign companies dealing with personal data of individuals in India.
- Obligations of data fiduciary (an entity or individual who collects and decides the means and purpose of processing personal data): processing will be subject to certain purpose, collection and storage limitations. For instance:
  - Personal data can be processed only for specific, clear and lawful purpose.
  - They must also institute mechanisms for age verification and parental consent when processing sensitive personal data of children.
  - Additionally, all data fiduciaries must undertake certain transparency and accountability measures such as:
    ✓ implementing security safeguards (such as data encryption and preventing misuse of data)
    ✓ instituting grievance redressal mechanisms to address complaints of individuals.
- Rights of the data principal (the individual whose data is being collected and processed): These include the right to:
  - obtain confirmation from the fiduciary on whether their personal data has been processed
  - seek correction of inaccurate, incomplete, or out-of-date personal data
  - have personal data transferred to any other data fiduciary in certain circumstances
  - restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn. It also provides a limited right to be forgotten.

often use pre-ticked boxes on consent while asking users regarding the acceptance to the terms and conditions.

Increasing sophistication of cyber-crimes: India is witnessing a significant change in the nature of cyber-crimes; it is now extremely organised and collaborative. Moreover, as the volume of data on internet is expanding exponentially and the spread of new technologies like artificial intelligence, internet of things, big data poses a threat of abuse and misuse of data.

The Personal Data Protection Bill, 2019

It seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. Its specific provisions are:

- Personal data (data that can identify an individual): The bill talks about various types of personal data, such as:
  - Sensitive personal data (related to finances, health, official identifiers, sex life, sexual orientation, biometric, genetics, transgender status, intersex status, caste or tribe, religious or political belief or affiliation)
  - Critical personal data (military or national security data and the government can define it from time to time)
  - General personal data- other than sensitive and critical personal data.
- Applicability: The Bill governs the processing of personal data by:
  - Government
  - companies incorporated in India
  - foreign companies dealing with personal data of individuals in India.
- Obligations of data fiduciary (an entity or individual who collects and decides the means and purpose of processing personal data): processing will be subject to certain purpose, collection and storage limitations. For instance:
  - Personal data can be processed only for specific, clear and lawful purpose.
  - They must also institute mechanisms for age verification and parental consent when processing sensitive personal data of children.
  - Additionally, all data fiduciaries must undertake certain transparency and accountability measures such as:
    ✓ implementing security safeguards (such as data encryption and preventing misuse of data)
    ✓ instituting grievance redressal mechanisms to address complaints of individuals.
- Rights of the data principal (the individual whose data is being collected and processed): These include the right to:
  - obtain confirmation from the fiduciary on whether their personal data has been processed
  - seek correction of inaccurate, incomplete, or out-of-date personal data
  - have personal data transferred to any other data fiduciary in certain circumstances
  - restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn. It also provides a limited right to be forgotten.

Challenges/ constraints in data protection

- India does not have capability for data localization i.e. to store data within country.
  - Most of the data storage companies are based abroad. They also export data to other jurisdiction making it difficult to apply Indian laws.
- There hundreds of private players are involved in data dynamics which makes it difficult to apply uniform data protection framework.
- It is usually difficult to trace the perpetrator invading the data privacy.
- **Grounds for processing personal data**: The Bill allows processing of data by fiduciaries only if consent is provided by the individual. However, in certain circumstances, personal data can be processed without consent. These include:
  - if required by the State for providing benefits to the individual
  - legal proceedings
  - to respond to a medical emergency
- **Social media intermediaries**: platforms with a larger number of users and having potential to impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.
  - According to official sources, while the process can be voluntary for users and can be completely designed by the company, it will decrease the anonymity of users and “prevent trolling”.
- **Data Protection Authority**: The Bill sets up a Data Protection Authority which may:
  - take steps to protect interests of individuals
  - prevent misuse of personal data
  - ensure compliance with the Bill.
- **Transfer of data outside India**: Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India.
  - Critical personal data can only be processed in India.
  - Personal data other than sensitive and critical personal data don’t have such localisation mandates.
- **Exemptions**:
  - The central government can exempt any of its agencies from the provisions of the Act:
    - in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states
    - for preventing incitement to commission of any cognisable offence (i.e. arrest without warrant) relating to the above matters.
  - Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as:
    - prevention, investigation, or prosecution of any offence
    - personal, domestic
    - journalistic purposes
- **Sharing of non-personal data with government**: The central government may direct data fiduciaries to provide it with any:
  - non-personal data

### Comparison of Personal Data Protection (PDP) Bill with EU’s General Data Protection Regulations (GDPR) 2018

#### Differences

- **Data transfer abroad**: Both PDP and GDPR give a government authority power to decide if data transfers can occur. However, while PDP doesn’t specify much details about other country’s “adequacy” in receiving data; GDPR takes this into account on basis of country’s rule of law, authorities etc.
- **Automated decision-making**: is process of making decision by automated means without any human involvement. It includes, for e.g., a company deciding credit score and profiling an individual for targeted advertising.
  - PDP requires an assessment in cases of large-scale profiling, but does not give the citizen the right to object to profiling, except in the cases of children. Whereas, the GDPR much more directly addresses personal harm from automated decision-making.
- **Personal data types**: To give special attention to particularly important types of data, India’s PDP categorises personal data much more explicitly.
  - Sensitive personal data: While GDPR doesn’t have separate localisation rules for this type of data, PDP doesn’t allow for sensitive personal data to be stored abroad & can only be processed abroad with authority approval.
  - Critical personal data: can never leave country for storage or processing.
- **Non-personal data**: PDP has allowed government to direct any entity handling data to provide them with non-personal data, or anonymised data. GDPR does not concern with processing of such anonymous information.

#### Similarities

- **Exceptions**: Both allow data processing for prevention, investigation, detection, or prosecution of criminal offences. Both also discuss “public security”, “defence”, and “judicial” proceedings.
- **Consent**: In both PDP and GDPR:
  - Consent carries similar meanings, with words like “free”, “specific”, and “informed”.
  - “Reasonable expectations” are provided for processing and collection.
  - They also both given special protection to children’s lack of ability to give consent.
- **Authorities**: European Data Protection Board in GDPR and Data Protection Authority in PDP have some similar duties.
California’s new privacy law - California Consumer Privacy Act (CCPA)

- It applies to businesses collecting information of Californians; not just to businesses that operate in the state. This means even Indian companies that have customers in California would have to comply with the law.

- Rights given by CCPA to California users:
  - Right to see what personal information businesses collect about them, and the purpose and process of collection.
  - Right to request and view what inferences the businesses make about them.
  - Right to see details about their personal information being sold or given to a third party and Right to opt out of having their data sold to third parties.
  - Parents have to give permission to companies before the companies can sell the data of their children under the age of 13 to third parties.
  - Right to make businesses delete one’s personal information.
  - Right to get a copy of the collected personal information for free.

- Companies will need to set up web pages and phone numbers to take requests. Users also may begin to see a new button on websites stating “Do Not Sell My Personal Information”.

Amendments to other laws: The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data.

Offences: Offences under the Bill include:
  - processing or transferring personal data in violation of the Bill
  - failure to conduct a data audit
  - Re-identification and processing of de-identified personal data without consent.

Criticism of the bill

- A report from the IT Ministry’s Artificial Intelligence (AI) Committee tasked with recommending policy frameworks on “cyber security, safety, legal and ethical issues”, contradicts foundational aspects of the Bill, such as:
  - India should maintain free flow of data: The report states that India has been one of the biggest beneficiaries of the global data flows being the world’s largest sourcing destination for the IT-BPM (Business Process Management) services. Limitations on the free and open flow of data can seriously hinder the ability of an economy to remain competitive in the modern globalised world.
  - Focus should be placed on implementation and enforcement instead of over-regulation. Legislation alone is not enough unless supported by an adequate implementation ecosystem including an effective grievance redressal system and user awareness.
  - Sectoral entities are more appropriate regulators than an overarching authority.

- It is also contended that security and government access are not achieved by mere localisation. Even if the data is stored in the country, the encryption keys may still be out of reach of national agencies.

- There are three significant departures in the current bill from the draft Bill prepared by the Justice B N Srikrishna committee in 2018.
  - Data Protection Authority’s composition is dominated by the government, in contrast with the diverse and independent composition as suggested in the committee’s draft.
  - There is a blanket power of exemption from all provisions of the law (including access to personal data without consent, citing national security, investigation and prosecution of any offence, public order) in favour of a government agency. This could amount to surveillance.
  - There is an attempt to control social media by reserving a right of access without consent of non-personal data or anonymized data.
    - Data is a person’s individual fundamental right and that is being abridged without following the strict constitutional parameters.

- The draft Bill prepared by the Justice B N Srikrishna committee called for a copy or mirror of all personal data to be stored in the country. This recommendation was severely criticised by foreign technology companies that store most of Indians’ data abroad and even some domestic start-ups. So, on a positive side, the approved Bill removes this stipulation by requiring individual consent for data transfer abroad.
  - However, similar to the draft, Bill still requires sensitive personal data to be stored only in India. It can be processed abroad only under certain conditions including approval of a Data Protection Agency (DPA). Moreover, critical personal data must be stored and processed in India.
From Market perspective:

- Mandates of the Bill like Data localisation, data fiduciary responsibility, steep fines etc. are likely to have repercussions for industries across the board - from retail to aviation, manufacturing to automobiles, and even a local grocer if he stores one’s details in a digital format.
- Technology giants like Facebook and Google are concerned with a fractured Internet (or a “splinternet”), where the domino effect of protectionist policy will lead to other countries following suit. Opponents say protectionism may backfire on India’s own young start-ups that are attempting global growth, or on larger firms that process foreign data in India, such as Tata Consulting Services and Wipro.
- Another contentious part of the bill is government’s access to non-personal data. A business entity may have non-personal data such as financial data, business strategy data, future projections data, etc., that is not personal but necessary from the company’s point of view. Any business entity would not be comfortable in sharing all such data with the government.

Conclusion

Considering the data privacy as the fundamental right of a citizen and economic downturns of the potential breaches in data, government need to reconsider the above pending issues. A robust Personal data protection law is the need of the hour. Due importance needs to be given on public awareness, better implementation and regulation and efficient grievance redressal as well.
Summary

Data is any collection of information that is stored in a way so computers can easily read them. Companies, governments, and political parties find this data valuable because they can use it to find the most convincing ways to advertise or shape our opinions online.

Data protection is the process of protecting the personal data and aims to strike a balance between individual privacy rights while still allowing data to be used for myriad purposes.

India does not have any dedicated legal framework for data protection. Personal data protection Bill, 2019 was introduced recently in Lok Sabha. The draft Bill, 2018 was prepared by a high-level expert committee headed by former SC judge B.N. Srikrishna.

About the Personal data protection Bill, 2019

It deals with guidelines on collection, storage and processing of personal data, the consent of individuals, penalties and compensation, and a code of conduct.

- It has a provision where the person shall have the right to restrict or prevent continuing disclosure of personal data.
- Sensitive personal data which includes passwords, financial-and health data, sexual orientation etc. can be processed only with the explicit consent of the person.
- There is a provision for the centre to notify categories of data as critical, which will only be processed in a server located in India.
- The central government can exempt any of its agencies from the provisions of the Act in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states.
- It sets up a Data Protection Authority which may take steps to protect interests of individuals, prevent misuse of personal data and ensure compliance with the Bill.

Criticism of the bill

- IT Ministry’s Artificial Intelligence (AI) Committee observes:
  - India should maintain free flow of data
  - Focus should be placed on implementation and enforcement instead of over-regulation.
  - Sectoral entities are more appropriate regulators than an overarching authority.
- Even if the data is stored in the country, the encryption keys may still be out of reach of national agencies.
- Departures in the current bill from the draft Bill prepared by the Justice B N Srikrishna committee in 2018.
  - Data Protection Authority’s composition is dominated by the government
  - There is a blanket power of exemption from all provisions of the law (including access to personal data without consent, citing national security, investigation and prosecution of any offence, public order) in favour of a government agency. This could amount to surveillance.
- There is an attempt to control social media by reserving a right of access without consent of non-personal data or anonymized data.
- Similar to the draft, the Bill still requires sensitive personal data to be stored only in India.
- From Market perspective:
  - Mandates of the Bill like Data localisation, data fiduciary responsibility, steep fines etc. are likely to have repercussions for industries across the board
  - Apprehensions of a fractured Internet (or a “splinternet”), where the domino effect of protectionist policy will lead to other countries following suit.
  - Government’s access to non-personal data: Any business entity would not be comfortable in sharing all such data such as financial data, business strategy data, future projections data, etc. with the government.

Conclusion

Considering the data privacy as the fundamental right of a citizen and economic downturns of the potential breaches in data, government need to reconsider all the above pending issues. A robust Personal data protection law is the need of the hour. Due importance needs to be given on public awareness, better implementation and regulation and efficient grievance redressal as well.