CoWIN data leak

Why in news?

In one of the largest data breaches in India, data of several Indians vaccinated against Covid-19 was leaked on a Telegram bot.

What is the background of the issue?

- **Data leak –** The leak was of data stored on the CoWIN portal.
- The portal is a government-funded online platform that was created to record personally identifiable information about those vaccinated against Covid-19.
- **Personal info –** It includes name, gender & birth details, as well as Aadhaar numbers, PAN cards, passport numbers, voter ids, and details of the vaccination centre in which a person was immunised.
- The data bot was offered by a Telegram channel called hak4learn, which frequently provides hacking tutorials.
- However, the telegram bot has now been taken down.

What is data protection?

- **Data protection –** It is the process of safeguarding important information from corruption, compromise or loss.
- The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates.
- There is also little tolerance for downtime that can make it impossible to access important information.
- Consequently, a large part of a data protection strategy is ensuring that data can be restored quickly after any corruption or loss.

What is the difference between personal data & non-personal data?

Personal Data	Non-Personal Data
• Personal data is any information that relates to an identified or identifiable living individual. • Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.	• In its most basic form, non-personal data is any set of data which does not contain personally identifiable information. • This in essence means that no individual or living person can be identified by looking at such data.

What is CoWIN?

- **eVIN –** India has been using a vaccine intelligence system called eVIN, which provides real-time feedback of vaccine stocks, power outages, temperature fluctuations etc.
- **Covid vaccination –** CoWIN is essentially an extension of eVIN and is a cloud-based IT solution for planning, implementation, monitoring, and evaluation of Covid-19 vaccination in India.
- It displays booking slots of COVID-19 vaccine available in the nearby areas and can be booked on the website.

Was there a really a data breach?

- The Ministry of Electronics and Information Technology has not explicitly clarified whether or not the CoWIN database was breached recently or in the past.
- While the Ministry said that it has adequate security measures to protect CoWIN's database, at no point has it said the database itself has not been impacted.
- This only leaves the possibility that the Telegram bot was not scraping data from CoWIN in real time.

What is the Centre's defence?

- **Data access –** The Ministry of Health press release first lays out the three ways in which data on CoWIN can be accessed:
    1. A user can access their data on the portal through a onetime password (OTP) sent to their mobile number.
    2. A vaccinator can access data of a person, and the CoWIN system tracks and records each time an authorised user accesses the system.
    3. Third party applications that have been provided authorised access of CoWIN APIs can access personal level data of vaccinated people after OTP authentication.
- Then it claims that without an OTP, data cannot be shared with the Telegram bot.
- However, there is one API that has a feature of sharing the data by using just a mobile number.

API stands for Application Programming Interface and it refers to any software with a distinct function.

- This API only accepts requests from a trusted API that has been whitelisted by the CoWIN system.
- Hence, there is no clarity on what this trusted API does and why it has been afforded the privilege of bypassing the entire OTP mechanism.

What are the implications of the breach?

- The Health Ministry has asked CERT-In to look into this issue and submit a final report.
- The Ministry is yet to receive a final report on the incident from CERT-In on the issue.

- As such, it would be premature to disprove a breach until CERT-In explicitly states that in its report.

National Data Governance policy has been finalised that will create a common framework of data storage, access and security standards across all of the government.

What are current legal provisions for privacy and data leaks?

- The data protection bill remains in draft stage.
- Every draft is more diluted than the previous one and gives more relaxation to the state.
- The state needs to gain the trust of users. And it is failing miserably there.

What is the way forward?

- The problem is that the level of awareness about all this is very low in India and there is so much potential for misuse.
- The government is trying to project itself as a big player in digital technology.
- However, it does not have the capacity or competence at this point of time to protect its own database.
- If there is no protection provided to users, we will continue to see such data leaks.

Quick Facts

CERT-In

- The Indian Computer Emergency Response Team (CERT-In) is the nodal agency for responding to computer security incidents as and when they occur.
- The CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.
- CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) and works
- To detect malicious programmes and free tools to remove the same.
- To provide cyber security tips and best practices for citizens and organisations.

References

1. The Indian Express | CoWIN data 'leak'
2. The Wire | Two Days After CoWIN Data Leak Report, Concerns Mount

SHANKAR IAS PARLIAMENT
Information is Empowering