Virtual Private Network (VPN)

May 9, 2022

In news– **VPN service providers are up in arms against a new directive of** the Indian Computer Emergency Response Team or **Cert-In**, a wing of the Ministry of Electronics and Information Technology, **that mandates they must maintain all customer data for five years.**

What is the issue?

- **As per the directive, Cert-In has asked VPN service providers to maintain for five years or longer details such as the validated names of their customers**, the period for which they hired the service, the IP addresses allotted to these users, the email addresses, the IP addresses and the time stamps used at the time of registration of the customers.
- **Cert-In also wants VPN service providers to maintain data such as the purpose for which the customers used their services,** their validated addresses and contact numbers, and the ownership pattern of the customers.
- One of the main reasons that Cert-In provided for seeking these details is that **it will help to effectively trace anti-social elements and cybercriminals indulging in various nefarious activities online.**
- **These details are necessary to prevent incitement or commission of any "cognisable offence using computer resources** or for handling of any cyber incident" which may lead to any disturbance in the "sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order".
- As per VPN service providers, **the new directive would mean a total loss of privacy for the users**—one of the most important unique selling points of such services.

- The main reason why privacy or anonymity is important for both **VPN service** providers and users is that **it helps to avoid being tracked, mostly by websites and cybercriminals**.
- Since VPN masks the location of a device from everyone, **it also prevents government and law enforcement agencies from accurately identifying the location.**
- VPN has also been of vital importance in countries that try to suppress dissent. **By using VPNs, dissidents are able to spoof their location and stay safe.**

What is Virtual Private Network (VPN)?

- Virtual Private Network is a way to extend a private network using a public network such as the internet.
- A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host.
- This means that if one surf online with a VPN, the VPN server becomes the source of your data.
- A virtual private network, when switched on, essentially creates a safe network within the larger global network of the internet and masks the IP address of the user by rerouting the data.
- Acting as a tunnel, a VPN takes data originating from one server and masks it in a different identity before delivering it to the destination server.
- In essence, a VPN creates several proxy identities for your data and delivers it safely without disturbing the content of the data.
- This means the Internet Service Provider (ISP) and other third parties cannot see which websites a person visit or what data he/she send and receive online.