Sansad TV Perspective: New VPN Rules

In the series Sansad TV Perspective, we bring you an analysis of the discussion featured on the insightful programme 'Perspective' on Sansad TV, on various important topics affecting India and also the world. This analysis will help you immensely for the IAS exam, especially the mains exam, where a well-rounded understanding of topics is a prerequisite for writing answers that fetch good marks.

In this article, we feature the discussion on the topic: New VPN Rules

Anchor: Vishal Dahiya

Participants:

1. Karmesh Gupta: Co-Founder and CEO, Wi-Jungle
2. Manoj Dhanda: Founder and CTO, MicroHost
3. Khushboo Jain: Advocate in Cyber Law

Context: In April 2022, Computer Emergency Response Team-India (CERT-In) released new VPN norms for VPN (Virtual Private Network) and cloud service providers as well as data centres working in India. The new VPN rules will come into effect by 27th, June 2022. New VPN rules are aimed to enhance the cyber security of India.

Understanding the VPN Technology:

A VPN (Virtual Private Network) is a network service that creates a safe, encrypted online connection. It disguises its user identity and does not allow its user activities to be tracked. Internet users may use a VPN to give themselves more privacy and anonymity online or circumvent geographic-based blocking and censorship. In other words, VPN hides user IP addresses from corporations, government agencies, and would-be hackers.

Significance of VPN:

- **Security on Public Wi-Fi:** A VPN protects user data while they are on other public networks, and hides user browsing history, banking information, account passwords, and more from ill-intentioned internet users.
- **Data Privacy from the Apps and Services:** A VPN prevents apps and websites from attributing user behaviour to your computer's IP address. It can also limit the collection of user location and browser history.
- **Data Privacy from Internet Service Providers:** Internet service providers can access all user internet data and browse history. This data can be collected and sold to advertisers and can be

dangerous in the wrong hands in the case of a data breach. A VPN can help obscure user IP addresses from Internet Service Providers (ISP).

- **Data Privacy from the Government:** A VPN protects user data and activities to be tracked by government agencies.
- **Access to Any Content:** VPNs spoof user location, making it seem as if a user is browsing from another place. That means users can access any data which is restricted in its local network.
- **Security When Working Remotely:** VPN provides encryption features. Encryption means putting data into a coded format so its meaning is obscured, allowing users to keep confidential information safe.

Need for VPN Regulation:

- A VPN can be used to disguise identity and location as well as to get access to restricted content, hence it is often used by cyber criminals to hide their identity and location. Similarly, it is used to watch banned content (videos, movies, text, pornography, etc.) that can hamper social order and national security.
- Cyber attackers use even multi-layered VPNs to hide their identity and location to target common users, banks, and other critical infrastructures of the country. This makes it very hard to catch cyber culprits by law enforcement agencies.
- VPN service is an exponentially growing sector in India, in 2020 there will be 45 million VPN users in India which will grow by 650 percent in 2022.
- Due to the lack of VPN regulations, India is becoming a safe haven for cyber-criminals.

In the light of the above points, CERT-In released new VPN guidelines to ensure India's cyber security.

Provisions of New VPN Rules:

- VPN service providers along with data centres and cloud service providers are supposed to store information such as names, e-mail IDs, contact numbers, and IP addresses (among other things) of their customers for a period of five years.
- Such entities are required to report cyber security incidents to CERT-In within 6 hours.
- CERT-In can seek information from VPN service providers in case of cyber security incidence on a case-to-case basis to discharge its security obligations to enhance cyber security in India.

Read more about Cyber Crimes in the linked article.

Objections raised against New VPN Rules:

- The VPN service provider industry argues that privacy is the main selling point of VPN services, and new VPN rules would be in breach of the privacy cover provided by VPN platforms.

- The new rules are overreaching and so broad as to open up the window for potential abuse and there is the possibility of potential misuse by the government and its agencies to suppress dissent.
- Some VPN service providers argue they use RAM-only servers that do not have hard disks that need to maintain a log of user data.
- Some VPN service providers also argued that they are not obliged to abide by Indian law as their servers are located out of India.

Cross Argument Against Objections:

- The CERT-In said in its rules that "It will seek information from VPN service providers in case of cyber security incidence on a case-to-case basis to discharge its security obligations to enhance cyber security in India". This means it will not have any plug-in to track the activities of every user in Indian cyberspace. Information will be asked to handle cases of cyber security only.

Conclusion:

Digital technology and usage of the internet have grown exponentially in the world as an integral part of modern life as well. All devices connected to the internet are part of a large network of devices such as computers, mobile phones, etc. A VPN is significant for the safe network access and privacy of internet users. On the other hand, VPN is a double-edged sword as it can be misused by cyber criminals and prevent law enforcement agencies from operating efficiently. In this context, new VPN rules will help to end the golden age of criminal VPN usage.