Compliance, Security, and Sovereignty

Posted at: 07/05/2025

The Future of Satellite Communication in India: Compliance, Security, and Sovereignty

Introduction

India's Department of Telecommunications (DoT) has introduced stricter guidelines for satellite communication services to enhance national security and promote digital sovereignty. These guidelines apply to companies like Starlink, Amazon's Kuiper, and Jio, and include new requirements related to data localisation, national security, and indigenous technologies such as NavIC.

Key Compliance Requirements for Satellite Communication Companies

1. **Local Manufacturing**

   - Companies must submit a phased manufacturing plan to indigenise **20% of the ground segment** within five years.

2. **Data Localisation**

   - All satellite communication data must be stored **within India** to enhance data security and control.

3. **NavIC Integration**

   - Integration of **NavIC**, India's regional navigation system, is mandatory by **2029**.

4. **Website Blocking Mechanism**

   - Satellite companies must enable systems to block **government-identified websites**.

5. **Cooperation with Law Enforcement**

- Companies must share **metadata** with security agencies upon request.

Enhanced Data Localisation and Security Measures

1. **No Foreign Routing**

   - Operators must ensure that Indian user traffic is not routed through **foreign gateways** or space systems.

2. **No Data Mirroring Abroad**

   - Operators are prohibited from **mirroring Indian data** on foreign servers.

3. **Decryption Ban Outside India**

   - Operators must ensure **Indian telecom data** is not decrypted outside India.

4. **India-Based Infrastructure**

   - Data centres and monitoring systems must be located **within India**.

National Security and Law Enforcement Cooperation

1. **Service Restrictions**

   - Satellite services must be restricted in emergencies or conflict zones.

2. **Security Clearances**

   - Separate **security clearances** are required before launching voice or data services.

3. **Special Monitoring Zones**

   - Monitoring is mandatory in **border areas** and coastal regions up to **200 nautical miles**.

4. **Real-Time Tracking**

    ○ Operators must provide **real-time tracking** of user terminals.

Strategic Intent

These guidelines aim to achieve:

- **Digital sovereignty** and control over India's telecom infrastructure.

- **Enhanced national security** by preventing foreign interference.

- **Promotion of indigenous technologies** like NavIC.

- **Boosting local manufacturing** in telecom.

Conclusion

India's new satellite communication guidelines reflect the country's focus on enhancing national security, ensuring digital sovereignty, and promoting indigenous technology. These regulations will shape the operational landscape for satellite service providers and are important for discussions on national security, digital infrastructure, and technology in India.