

VPN Regulation in India, Government Weighs Stricter Rules for VPN Providers

July 3, 2026 • vajiramandravi.com



VPN Regulation in India Latest News

- The Centre is working on an **expansive legal framework** to regulate Virtual Private Network (VPN) providers. The proposed rules could require VPN companies to establish a local presence in India and appoint compliance officers to liaise with the government.
- The primary concern driving this: VPNs are increasingly being used to bypass the government's blocking of apps and online content.

What Is a VPN and Why Does It Worry the Government

- A VPN lets users **mask their IP address** and route their internet traffic through servers located elsewhere, making it appear as if the traffic originates from another country while hiding the user's real location.
- This creates two features the government finds problematic:

- **Bypassing censorship:** India's blocking orders require companies to geo-block content within India's jurisdiction. But by connecting through a VPN server in, say, the US, a user can still access content blocked in India.
- **Anonymity:** VPNs allow anonymous browsing and are widely regarded as privacy-enhancing tools.
- The scale of the tension is clear from India's expanding censorship: over 24,000 blocking orders in 2025, up from over 12,000 in 2024.
- When the Centre temporarily blocked Telegram before the NEET-UG retest, Proton VPN reported daily sign-ups from India jumping over 120% — illustrating exactly why VPNs “defeat the purpose” of blocking, in the government's view.

What the New Framework Could Require

- According to senior officials, the proposed rules could require VPN operators to:
 - Establish offices in India.
 - Hire compliance officers to address government grievances.
 - Face penal consequences, including possible jail terms for local employees, in case of non-compliance.
- These requirements mirror obligations already imposed on large social media companies under India's Information Technology (IT) Rules, 2021.
- The core goal is to have a local point of contact the government can direct to block access to prohibited content.

The Backstory: The 2022 Cert-In Directive

- This is not the first attempt to regulate VPNs.
- In 2022, the Indian Computer Emergency Response Team (Cert-In) issued a controversial directive requiring VPN providers (along with data centres and cloud service providers) to store extensive customer data — names, email IDs, contact numbers, and IP addresses — for a period of five years.
- Why a new law is now felt necessary: There is an implicit acknowledgement that the 2022 directive did not yield satisfactory results.
- As per analysts, VPN companies “simply refused to comply,” so a full-fledged law is being considered.

The Industry's Response Servers Moved Out

- The 2022 directive backfired in a telling way. Rather than comply, major VPN operators — Proton VPN, NordVPN, ExpressVPN, and Surfshark — **removed their physical servers** from India and began routing Indian traffic through Singapore.
- Proton VPN was blunt at the time, calling it an “invasive mass surveillance law” and saying it had no choice but to pull its servers out of Indian jurisdiction.
- This episode highlights the core enforcement challenge: because VPN companies can operate entirely from outside India, forcing compliance is difficult — which is precisely why the government now wants a mandatory local presence.

The Underlying Tension: Security vs. Privacy

- The story sits at the intersection of two competing concerns:
 - **The government's position:** VPNs undermine lawful content-blocking and enable circumvention of orders issued on security and other grounds; a local, accountable presence is needed for enforcement.
 - **The privacy concern:** VPNs are legitimate privacy-enhancing tools, and data-retention or localisation mandates raise fears of mass surveillance and erosion of user anonymity.

Conclusion

- The proposed VPN framework is the government's second, tougher attempt to bring a hard-to-regulate technology under its control.
- Where the 2022 Cert-In data-retention directive largely failed — pushing providers to simply relocate their servers abroad — the new approach borrows the IT Rules playbook: mandate a local office, a compliance officer, and personal liability for employees.
- The move underscores India's expanding content-blocking regime, but it also reopens a fundamental debate.
- VPNs are both a tool for evading censorship and a legitimate shield for privacy. How the eventual law balances enforcement against the surveillance concerns raised by providers and civil society will be its real test.

Source: IE

Source: <https://vajiramandravi.com/current-affairs/vpn-regulation-in-india/>

© Vajiram & Ravi. For personal use only.