Understanding India's Internet Censorship Regime

Mains: *GS II – Governance| GS III Science and Technology*

Why in News?

India's digital ecosystem has grown exponentially over the past decade, positioning the country as one of the largest internet markets in the world and alongside this growth lies a complex and often opaque system of internet regulation and censorship.

What are the legal framework governing internet censorship?

- **Legal framework** – India's internet censorship is primarily governed by the Information Technology Act, 2000.
- Two key provisions —Section 69A and Section 79 of this act, empower the government to regulate online content.
- **Section 69A** allows the central government to issue directions to block public access to information on grounds such as national security, public order, and sovereignty.
- **Section 79** provides conditional immunity to intermediaries (including ISPs), provided they comply with government directives.
- Additionally, ISP licensing agreements mandate compliance with government-issued blocking orders.
- These agreements explicitly require ISPs to block websites as directed by authorities.
- **Judicial Intervention** – A critical judicial intervention came in the *Shreya Singhal vs. Union of India case*, where the Supreme Court upheld the constitutionality of Section 69A while emphasizing procedural safeguards.
- These include:
    - A review committee to oversee blocking orders.
    - The right of affected parties to be heard.
- Despite these safeguards, their practical implementation remains limited due to systemic opacity.
- **Opacity in the Blocking Process –** One of the most significant issues in India's censorship regime is the lack of transparency.
- Blocking orders issued under Section 69A are confidential, meaning:
    - ISPs cannot disclose the orders they receive.
    - Users are often unaware of why a website is inaccessible.
    - Website operators are not always informed or given an opportunity to respond.
- In contrast, blocking orders arising from copyright or trademark disputes are often made public through court proceedings.
- Occasionally, the government announces major blocking actions, such as the 2020 ban on 59 Chinese apps, including TikTok.

- However, most blocking decisions remain hidden from public scrutiny.

What are the technical mechanisms of website blocking?

- **DNS blocking (DNS Poisoning) –** The Domain Name System (DNS) translates human-readable domain names into IP addresses.
- ISPs can manipulate this process by returning incorrect IP addresses for blocked domains, effectively preventing users from accessing them.
- This technique is widely used in India due to its simplicity and low cost.
- **HTTP interception –** In this method, ISPs intercept unencrypted HTTP traffic and display a block page.
- However, this technique has become less relevant as most websites now use HTTPS.
- **SNI filtering –** For HTTPS connections, ISPs can inspect the Server Name Indication (SNI) field during the initial handshake.
- If the domain matches a blocked site, the connection is terminated before it is established.
- Among these, DNS blocking remains the dominant method used by Indian ISPs.
- **Empirical Insights, scale and nature of blocking –** A large scale study conducted in 2025 examined DNS-level censorship across six major and regional ISPs.
- The study analyzed approximately 294 million domains, representing nearly the entire visible domain space.
- **Key Findings:**
    - Total blocked domains identified – 43,083
    - Domains blocked by all six ISPs – Only 1,414
- This indicates a significant lack of uniformity in implementation.
- **Categories of blocked content:**
    - Piracy and copyright infringement websites.
    - Peer-to-peer file-sharing platforms.
    - Pornographic content.
    - Gambling websites.
    - Terrorism and militancy-related content.
- Notably, blocking consistency was highest for sensitive categories such as terrorism-related content.
    - **For instance**, domains like Weibo and certain politically sensitive publications were uniformly blocked across ISPs.

What are the inconsistencies across ISPs?

- **Unequal access to information** – A website blocked on one ISP may be accessible on another.
- **Arbitrary enforcement** – Some ISPs block additional domains without clear legal backing.
- **Non-compliance with unblocking orders** – Certain domains remain blocked even after official directives to restore access.
- Such inconsistencies undermine the stated objectives of censorship while disproportionately affecting users of stricter ISPs.
- **Arbitrary and Overbroad Blocking –** The study also revealed that many ISPs engage

in arbitrary blocking.
- This includes:
  - Blocking entire domains instead of specific URLs
  - Continuing to block domains without valid orders
  - Blocking potentially legitimate or harmless content
- Furthermore, the presence of malicious domains among blocked sites raises important questions.
- While blocking harmful domains may serve the public interest, the absence of transparency makes it impossible to distinguish between legitimate regulation and overreach.

What are the impact on fundamental rights and other challenges?

- **Freedom of speech and expression –** Article 19(1) (a) of the Constitution guarantees freedom of speech and expression.
- Arbitrary and opaque blocking restricts access to information and limits public discourse.
- **Right to information –** Access to information is a cornerstone of democracy.
- Inconsistent censorship creates an uneven information landscape, where access depends on the user's ISP.
- **Due process –** The lack of transparency and limited avenues for redress weaken procedural fairness.
- Affected parties often have no effective means to challenge blocking decisions.
- **Challenges in oversight and accountability –** Although procedural safeguards exist on paper, their effectiveness is limited:
  - Review committees lack transparency
  - Affected parties are rarely notified
  - No penalties for ISP non-compliance
  - This creates a system where accountability is minimal, and enforcement is uneven.

What are the reforms needed?

- **Transparency in blocking orders –** A publicly accessible database of blocked domains should be maintained, with exceptions only for sensitive cases such as national security or child protection.
- **Standardized implementation guidelines –** Clear technical and procedural guidelines should be issued to ensure uniform implementation across ISPs.
- **Strengthening oversight mechanisms –** Independent oversight bodies should be empowered to review blocking decisions and ensure compliance.
- **User and operator notification –** Website operators and users should be informed about blocking actions and provided with avenues for appeal.

What lies ahead?

- India's internet censorship regime reflects a complex interplay between legal authority, technical implementation, and administrative discretion. While the state has legitimate interests in regulating harmful content, the current system is marked by

inconsistency, opacity, and limited accountability.

- The variation in user experience across ISPs highlights a fundamental issue: censorship in India is not just about what is blocked, but how it is blocked and by whom. Without transparency and standardization, the system risks undermining both its regulatory objectives and the democratic values it seeks to protect.
- A reformed approach—grounded in openness, fairness, and uniformity—is essential to ensure that internet governance in India aligns with constitutional principles and the needs of a digital society.

Reference

[The Hindu| Censorship Regime in India]