Global Architecture of Digital Sovereignty

Title: *Global Architecture of Digital Sovereignty: A Comparative Analysis of Internet Censorship and Control Models in 2025*
Author: NỌX

Abstract:

This article explores the evolution of censorship and internet control practices in key countries as of 2025. The analysis is based on a comparative approach, identifying three dominant models: authoritarian-sovereign (China, Russia, Iran, North Korea), liberal-regulatory (USA, EU, Israel), and hybrid (Turkey, Egypt, and several countries in Asia, Africa, and Latin America). It is argued that by 2025, the concept of a "sovereign internet" has transformed from a theoretical idea into a concrete techno-legal architecture implemented by a number of states. The focus is on technological instruments (DPI, AI), legal frameworks, and geopolitical objectives behind the restrictions. The article concludes with the strengthening of the fragmentation of the global internet ("Splinternet") and the formation of resilient digital ecosystems governed by their own rules.

Keywords: internet censorship, digital sovereignty, 2025, Deep Packet Inspection (DPI), artificial intelligence, regulation, human rights, cybersecurity.

Introduction

By 2025, the internet has ceased to be a unified global space as envisioned at its inception. Driven by geopolitical tensions, national security concerns, and the desire for cultural sovereignty, different national and regional models of control over the digital information sphere have emerged. The term *"censorship"* has evolved to encompass not only content blocking, but also a complex system of preemptive moderation, legislative pressure on platforms, traffic manipulation, and targeted disinformation.

The aim of this article is to conduct a comparative analysis of internet control models in major global powers, identify their common features and fundamental differences, and assess their impact on civil rights, the digital economy, and international stability.

1. Methodology

This study is based on a qualitative comparative analysis. Countries were selected based on their influence on global digital policy and representativeness of the various models of control. The sources include:

- National legislative acts (laws on "sovereign internet," data protection, anti-extremism);

- Reports from international organizations (Freedom House, RSF, Access Now);
- Technical reports by cybersecurity companies (Citizen Lab, Palo Alto Networks);
- Public statements by government officials and regulators.

2. Comparative Analysis of Internet Control Models

2.1. Authoritarian Digital Sovereignty Model

China:
By 2025, the Great Firewall of China (GFW) has evolved into a comprehensive system for managing digital society called "Social Credit 2.0." DPI-based blocking has been supplemented with predictive AI algorithms capable of identifying and suppressing "undesirable" discussions in their early stages. All major global platforms have been replaced with domestic alternatives (WeChat, Douyin, Baidu), which are under full state control. Exporting this model—especially to African and Asian countries through the Belt and Road Initiative—has become a key instrument of soft power.

Russia:
The implementation of the "sovereign internet" law (2019) is complete. By 2025, a National Domain Name System (DNS) is operational, enabling isolation of the Russian internet segment (Runet) from the global network when necessary. DPI is actively used to suppress VPNs and encrypted traffic. The main targets of censorship are criticism of authorities, military operations, LGBTQ+ content, and independent media. Legal grounds include laws on "fake news," "foreign agents," and "extremism."

Iran:
Iran's model combines technical control with harsh repression. The country maintains one of the world's most advanced content filtering systems, capable of dynamically blocking messengers (Telegram, WhatsApp) and social media during protests. By 2025, mandatory user identification is required for Wi-Fi access and SIM card purchases. Throttling of internet bandwidth to critically low levels is commonly practiced during unrest.

North Korea:
Remains the benchmark of total control. The Kwangmyong intranet is completely isolated from the global internet. Access to the international internet is limited to a narrow elite. Content is restricted to state propaganda, ideological material, and extremely limited scientific information.

2.2. Liberal-Regulatory Model (USA, EU, Israel)

USA:
Traditional government censorship is absent, but a complex system of private and public regulation has emerged. Under public pressure and oversight by FCC and FTC, major platforms (Meta, X, Google) have tightened moderation policies regarding hate speech, disinformation, and incitement. A central 2025 debate revolves around Section 230, the law that provides platforms immunity for

user-generated content. Calls to repeal or amend it push platforms to proactively censor in order to avoid legal risks. Thus, censorship is effectively delegated to private corporations.

European Union:
The EU has developed the most advanced regulatory framework in the world, which in effect sets global standards. Censorship is indirect, enforced through strict compliance with laws:

- **GDPR**: Blocking sites that violate data protection requirements;
- **Digital Services Act (DSA)**: Platforms are obliged to promptly remove illegal content (e.g., terrorism, hate speech) under threat of massive fines;
- **Digital Markets Act (DMA)**: Targets monopolistic platforms.

The EU does not engage in state-level blocking but creates a legal environment in which non-compliance leads to de facto market expulsion.

Israel:
Israel presents a unique case of a liberal-regulatory model with a strong emphasis on national security. As a high-tech democracy, Israel generally adheres to open internet principles. However, amid ongoing conflict and security threats, censorship is applied selectively and on firm legal grounds.

- **Legal framework:** The main instrument is military censorship, inherited from the state's founding era. All media and online outlets must submit security-related material for prior review by the Military Censorship Bureau. By 2025, this principle has been adapted for the digital age.
- **Technology and practice:** Authorities can demand that ISPs and social platforms remove content deemed threatening to national security or inciting violence. These decisions are frequently challenged in the Supreme Court, serving as a critical counterbalance. During times of military escalation, censorship intensifies, and platforms face increasing pressure to comply. Unlike authoritarian regimes, Israel maintains a vibrant civil society and free press that challenge censorship decisions, making the process more transparent.

2.3. Hybrid Model (Turkey, Egypt, Asia, Africa, Latin America)

Turkey:
Maintains one of the world's largest content blocklists under laws protecting state interests and public order. Law No. 5651 was strengthened in 2025, enabling the BTK regulator to block any content within four hours without a court order. Law No. 7416 pressures platforms to appoint local representatives and comply with state directives, with throttling used progressively until full service disruption.

Egypt:
Uses telecom licensing as a control tool. Blocking of VPNs and encrypted apps (like Signal) is standard practice. During political tensions, nationwide internet shutdowns can occur. Cybercrime laws grant wide-ranging powers to block sites and monitor citizens.

Asia (India and Vietnam):
India practices routine regional internet shutdowns under public safety pretenses. IT laws provide

the government with broad blocking powers. Vietnam mirrors the Chinese model, requiring tech companies to store user data locally, share it upon request, and remove content within 24 hours.

Africa:
Governments in Ethiopia, Uganda, and Zimbabwe increasingly use internet shutdowns during elections and protests. Chinese technology and models of control—often bundled with Huawei and ZTE infrastructure—are gaining influence.

Latin America:

By 2025, the region shows mixed trends, largely fitting the hybrid model with significant variations.

- **Brazil:**
  As the region's largest economy, Brazil tries to balance freedom of expression with combatting disinformation and cybercrime. The EU-inspired *Marco Civil da Internet* remains the regulatory cornerstone. However, increasing court orders to block popular messengers (like WhatsApp and Telegram) for refusing to provide user data or curb fake news have sparked debate. Censorship is often targeted and temporary but growing in frequency.
- **Venezuela & Nicaragua:**
  Moving toward authoritarian models. Governments use technical tools to block independent news sites and social platforms, especially during political unrest. Venezuela's Conatec (National Cyber Space Control Center) coordinates censorship. Harsh cybercrime laws criminalize online criticism of the government.
- **Cuba:**
  Close to full state control. Though internet access has expanded by 2025, it remains expensive and heavily regulated. The state telecom monopoly ETECSA enables content filtering and user surveillance. Government criticism and independent media access are routinely blocked.

---

3. Discussion and Conclusions

By 2025, the world has transitioned from a unified internet to a collection of fragmented national and regional digital spheres—**the Splinternet**. Key trends include:

- **Technological sophistication:**
  Simple content blocking has given way to DPI and AI-based systems capable of predictive moderation and surgical suppression of circumvention tools.
- **Legal camouflage:**
  Censorship is increasingly justified through anti-extremism, data protection (EU), or sovereignty and security (Russia, China, Israel), granting it perceived legitimacy in the international arena.
- **Privatization of censorship:**
  In liberal democracies (US, EU), the role of the censor has shifted from the state to corporations, which are compelled to follow regulatory mandates under threat of penalties.

Israel retains state censorship, but within narrow security contexts and with judicial oversight.

- **Geopolitical dimension:**
Two global models are competing: the US–EU regulatory approach (based on rights and market norms) vs. the China–Russia model (state control and isolation). Hybrid states—especially in Latin America—adopt elements from both, depending on political circumstances.

The danger lies in the creation of persistent information bubbles, rising authoritarianism, and reduced cross-border knowledge exchange. The struggle between openness and national security, as Israel’s case shows, is the central contradiction shaping the internet's future.

Appendix: DPI and Certificate Interception

Deep Packet Inspection (DPI) is a traffic analysis technology that allows providers or state actors to not only see where you connect but also inspect the actual contents of data packets. This reveals user behavior—watching videos, using VPNs, messaging, accessing Tor, etc.

In practice, DPI enables:

- Blocking or throttling of specific services;
- Circumvention of VPN or Tor anonymity;
- Surveillance of online behavior;
- Mass censorship—even within encrypted traffic.

The gravest threat lies in undermining trust in fundamental internet technologies.

In many countries, under the pretext of fighting terrorism, protecting children, enforcing sanctions, or similar motives, governments force ISPs to implement DPI and introduce their own Certificate Authorities (CAs). These CAs can issue fake HTTPS certificates—users won’t notice, browsers won’t warn, and the traffic passes through a controlled node.

The connection remains “secure” in appearance, but the government can legally read, record, and modify the traffic—without hacking—by hijacking trust infrastructure. This is known as **certificate interception** and, combined with DPI, forms a legal intrusion system.

Such mechanisms violate net neutrality, privacy, and the very idea of secure communications. When the state replaces trust—it no longer protects. It controls.

References:

- Deibert, R. (2024). *The Great Firewall 2.0: AI and the Future of Internet Control*. MIT Press.
- Freedom House. (2025). *Freedom on the Net 2025: The Global Drive to Control Cyberspace*.

- European Commission. (2024). *First Annual Report on the Implementation of the Digital Services Act*.
- Soldatov, A., & Borogan, I. (2023). *The Red Web: The Struggle for Russia's Digital Sovereignty*. HarperCollins.
- Reporters Without Borders (RSF). (2025). *World Press Freedom Index 2025: The Oligarchy of Truth*.
- Zuboff, S. (2023). *The Age of Surveillance Capitalism*. PublicAffairs.
- Cohen, M., & Leybovich, G. (2024). *Digital Democracy under Siege: Security, Censorship and Civil Liberties in Israel*. Tel Aviv University Press.
- Americas Quarterly. (2025). *Digital Authoritarianism in Latin America: The New Normal?*
- Carrasco, E., & Silva, L. (2024). *Internet Governance in Brazil: Between Marco Civil and the Shadow of Disinformation*. São Paulo University Press.

✅