Arquitetura Global da Soberania Digital

Título: *Arquitetura Global da Soberania Digital: Análise Comparativa de Modelos de Censura e Controle da Internet em 2025*
Autor: NQX

Resumo:

Este artigo investiga a evolução das práticas de censura e controle da internet nos principais países do mundo até o ano de 2025. A análise adota uma abordagem comparativa que identifica três modelos dominantes: o autoritário-soberano (China, Rússia, Irã, Coreia do Norte), o liberal-regulatório (EUA, União Europeia, Israel) e o híbrido (Turquia, Egito e diversos países da Ásia, África e América Latina). Argumenta-se que, em 2025, o conceito de “internet soberana” deixou de ser teórico e passou a constituir uma arquitetura técnico-jurídica consolidada em vários Estados. O foco recai sobre instrumentos tecnológicos (DPI, IA), fundamentos legais e objetivos geopolíticos por trás das restrições. Conclui-se que há uma intensificação da fragmentação da internet global (*Splinternet*) e o surgimento de ecossistemas digitais resilientes com regras próprias.

Palavras-chave: censura na internet, soberania digital, 2025, Inspeção Profunda de Pacotes (DPI), inteligência artificial, regulação, direitos humanos, cibersegurança.

Introdução

Até 2025, a internet deixou de ser o espaço global unificado idealizado em sua origem. Conflitos geopolíticos, preocupações com segurança nacional e a busca por soberania cultural levaram à criação de modelos nacionais e regionais de controle do espaço digital. O conceito de “censura” evoluiu, passando a englobar não apenas o bloqueio de conteúdos, mas também sistemas complexos de moderação prévia, pressões legislativas sobre plataformas, manipulação de tráfego e desinformação direcionada.

Este artigo tem como objetivo realizar uma análise comparativa dos modelos de controle da internet em países influentes, identificando suas semelhanças, diferenças fundamentais e impactos sobre os direitos civis, a economia digital e a estabilidade internacional.

---

1. Metodologia

A pesquisa baseia-se em uma análise comparativa qualitativa. Os países foram selecionados com base em sua relevância na política digital global e representatividade dos modelos analisados. As fontes incluem:

- Leis nacionais (sobre “internet soberana”, proteção de dados, combate ao extremismo);
- Relatórios de organizações internacionais (Freedom House, Repórteres Sem Fronteiras, Access Now);
- Relatórios técnicos de empresas de cibersegurança (Citizen Lab, Palo Alto Networks);
- Declarações públicas de autoridades e órgãos reguladores.

---

2. Análise Comparativa de Modelos de Controle da Internet

2.1. Modelo Autoritário de Soberania Digital

China:
Até 2025, o Grande Firewall evoluiu para um sistema abrangente de controle da sociedade digital, chamado “Crédito Social 2.0”. O bloqueio via DPI foi complementado com algoritmos preditivos de inteligência artificial, capazes de identificar e interromper discussões “indesejadas” em estágio inicial. As plataformas internacionais foram substituídas por equivalentes nacionais (WeChat, Douyin, Baidu), sob controle estatal total. A exportação desse modelo, especialmente por meio da iniciativa “Belt and Road”, tornou-se ferramenta estratégica de influência em países da África e Ásia.

Rússia:
A implementação da lei da “internet soberana” (2019) foi concluída. Em 2025, está em funcionamento um sistema nacional de DNS que permite isolar a Runet da internet global, quando necessário. O DPI é usado para bloquear VPNs e tráfego criptografado de forma seletiva. Os principais alvos da censura incluem críticas ao governo, operações militares, conteúdo LGBTQ+ e a mídia independente. As bases legais envolvem leis sobre “notícias falsas”, “agentes estrangeiros” e “extremismo”.

Irã:
O modelo iraniano combina controle técnico com repressão severa. O país possui um dos sistemas de filtragem mais avançados do mundo, capaz de bloquear dinamicamente mensageiros como Telegram e WhatsApp, além de redes sociais durante protestos. Em 2025, é obrigatória a identificação de usuários para acesso ao Wi-Fi ou compra de cartões SIM. A prática do *throttling* (redução extrema da velocidade da internet) é amplamente empregada.

Coreia do Norte:
Permanece como exemplo de controle absoluto. A rede Kwangmyong é completamente isolada da internet global. O acesso à rede internacional é restrito a uma elite mínima. O conteúdo disponível é composto principalmente por propaganda estatal, materiais ideológicos e dados científicos limitados.

2.2. Modelo Liberal-Regulatório (EUA, UE, Israel)

Estados Unidos:
Não existe censura estatal clássica, mas há um sistema sofisticado de regulação pública e privada. Sob pressão de órgãos como FCC e FTC, as grandes plataformas (Meta, X, Google) reforçaram políticas de moderação contra discurso de ódio, desinformação e incitação à violência. O debate central em 2025 envolve a Seção 230, que garante imunidade legal às plataformas por conteúdos de terceiros. Propostas de revogação ou revisão da norma incentivam ações preventivas por parte das empresas, resultando em censura indireta.

União Europeia:
A UE criou a estrutura regulatória mais avançada do mundo, estabelecendo padrões globais de fato. A censura se dá de forma indireta por meio de obrigações legais rigorosas:

- **RGPD:** bloqueio de sites que não atendem a normas de proteção de dados;
- **DSA (Lei de Serviços Digitais):** obriga plataformas a removerem rapidamente conteúdos ilegais (terrorismo, discurso de ódio), sob risco de multas elevadas;
- **DMA (Lei dos Mercados Digitais):** visa combater plataformas dominantes.

A UE não realiza bloqueios estatais diretos, mas impõe um ambiente legal que torna insustentável a permanência de plataformas que descumpram as regras.

Israel:
Exemplo singular de modelo liberal com foco acentuado na segurança nacional. Como democracia tecnológica, Israel adota princípios de internet aberta. Contudo, em contextos de conflito, aplica censura pontual com base legal:

- **Base legal:** O principal instrumento é a censura militar, existente desde a fundação do Estado. Todos os meios de comunicação — inclusive digitais — devem submeter conteúdos ligados à segurança ao órgão censor para análise prévia. Em 2025, essa prática foi adaptada ao contexto digital.
- **Tecnologia e prática:** O governo pode exigir a remoção de conteúdos considerados ameaçadores à segurança nacional ou que incitem à violência. Essas decisões frequentemente são contestadas na Suprema Corte, atuando como contrapeso. Durante operações militares, a censura tende a se intensificar. Diferente de regimes autoritários, Israel mantém imprensa livre e sociedade civil ativa, garantindo transparência.

2.3. Modelo Híbrido (Turquia, Egito, Ásia, África e América Latina)

Turquia:
Mantém um dos maiores cadastros de bloqueios do mundo, com base em leis de proteção ao Estado e segurança pública. A Lei n.º 5651, reforçada em 2025, autoriza o órgão regulador BTK a bloquear conteúdo em até 4 horas sem ordem judicial. A Lei n.º 7416 obriga plataformas a nomear representantes locais e cumprir determinações oficiais; em caso de descumprimento, aplica-se *throttling* progressivo até a total inacessibilidade.

Egito:
Utiliza o licenciamento de operadoras de telecomunicações como ferramenta de controle. O

bloqueio de VPNs e aplicativos criptografados (como Signal) é prática padrão. Em momentos de tensão política, o acesso à internet pode ser suspenso em nível nacional. A legislação sobre crimes cibernéticos concede amplos poderes de censura e vigilância estatal.

Ásia (Índia e Vietnã):
A Índia adota cortes seletivos de internet em estados específicos por razões de segurança. Suas leis concedem poder amplo ao governo para bloquear conteúdo. O Vietnã segue o modelo chinês, obrigando empresas tecnológicas a armazenar dados localmente, fornecer informações às autoridades sob demanda e remover conteúdo em até 24 horas.

África:
Países como Etiópia, Uganda e Zimbábue utilizam cortes temporários de internet durante eleições e protestos. Cresce a influência de tecnologias e modelos de controle chineses — frequentemente fornecidos com equipamentos da Huawei e ZTE.

América Latina:

Em 2025, observa-se diversidade de abordagens, geralmente dentro do modelo híbrido, com variações significativas.

- **Brasil:**
  A maior economia da região tenta equilibrar liberdade de expressão com o combate à desinformação e ao cibercrime. A Lei Marco Civil da Internet, inspirada na UE, continua sendo a base regulatória. No entanto, aumentam decisões judiciais ordenando o bloqueio de mensageiros como WhatsApp e Telegram por descumprirem ordens de fornecimento de dados ou combate a fake news.
- **Venezuela e Nicarágua:**
  Migrando para modelos autoritários. Governos usam meios técnicos para bloquear portais de notícias independentes e redes sociais, especialmente durante crises políticas. Na Venezuela, o Conatec (Centro Nacional de Gestão do Ciberespaço) coordena a censura. Leis sobre "cibercrimes" criminalizam críticas ao governo na internet.
- **Cuba:**
  Modelo próximo ao controle estatal absoluto. Embora o acesso tenha aumentado em 2025, continua caro e monitorado. A ETECSA, operadora estatal, permite ao governo filtrar conteúdo e monitorar usuários. Críticas ao regime e acesso à imprensa independente são sistematicamente bloqueados.

---

3. Discussão e Conclusões

Em 2025, o mundo passou de uma internet global unificada para múltiplos espaços digitais fragmentados — a **Splinternet**. Tendências-chave:

- **Sofisticação tecnológica:**
  Bloqueios simples foram substituídos por sistemas avançados com DPI e IA, capazes de moderação preditiva e repressão de ferramentas de anonimato.
- **Justificativa legal:**
  A censura é frequentemente embasada em combate ao extremismo, proteção de dados (UE),

soberania nacional (China, Rússia) ou segurança (Israel), conferindo-lhe aparente legitimidade internacional.

- **Privatização da censura:**
  Em democracias liberais (EUA, UE), empresas privadas passaram a exercer o papel de censores, sob risco de sanções. Em Israel, a censura continua estatal, mas com limitação judicial e foco em segurança.
- **Dimensão geopolítica:**
  Confrontam-se dois modelos globais: o dos EUA/UE (regulação por direitos e mercado) e o da China/Rússia (controle estatal e isolamento). Países da "faixa híbrida", como muitos latino-americanos, adotam elementos de ambos conforme conveniência política.

Risco principal: criação de bolhas informativas, fortalecimento do autoritarismo e restrição ao intercâmbio transnacional de conhecimento.
O dilema entre abertura e segurança nacional — como evidenciado por Israel — será o ponto central que definirá o futuro da internet.

Apêndice: DPI e Interceptação de Certificados

DPI (Inspeção Profunda de Pacotes) é uma tecnologia de análise de tráfego que permite examinar não só os destinos acessados, mas também o conteúdo transmitido.
Revela se o usuário assiste vídeos, usa Tor/VPN, envia mensagens etc.

Na prática, o DPI permite:

- Bloquear ou reduzir a velocidade de serviços específicos;
- Romper o anonimato de VPN e Tor;
- Monitorar comportamentos online;
- Aplicar censura massiva — até mesmo em tráfego criptografado.

A maior ameaça é a destruição da confiança nas tecnologias fundamentais da internet.

Em muitos países, sob pretextos como "combate ao terrorismo" ou "proteção infantil", governos exigem uso de DPI e implementam **autoridades certificadoras (CA)** estatais.
Isso permite substituir certificados HTTPS por falsos — sem alertas do navegador —, desviando tráfego para servidores controlados.

Formalmente, a conexão parece segura, mas o governo pode ler, registrar e até alterar os dados — sem invadir, apenas manipulando a confiança.
Isso é conhecido como **interceptação via certificados falsos**. Combinada com DPI, constitui uma infraestrutura legal de invasão à privacidade.

Viola a neutralidade da rede, compromete a confidencialidade e subverte o princípio de segurança digital.
Quando o Estado substitui a confiança — ele não protege. Ele controla.

Fontes:

- 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*
- Comissão Europeia. (2024). *Relatório Anual sobre a Lei de Serviços Digitais*
- Soldatov, A., Borogan, I. (2023). *The Red Web*. HarperCollins
- Repórteres Sem Fronteiras. (2025). *Índice Mundial de Liberdade de Imprensa*
- Zuboff, S. (2023). *A Era do Capitalismo de Vigilância*. PublicAffairs
- Cohen, M., Leybovich, G. (2024). *Democracia Digital Sob Cerco*. Tel Aviv University Press
- Americas Quarterly. (2025). *Autoritarismo Digital na América Latina*
- Carrasco, E., Silva, L. (2024). *Governança da Internet no Brasil*. São Paulo University Press

---