Policy Brief: Perspectivas sobre o bloqueio de conteúdo na Internet

Setembro de 2025

Resumo executivo

Imagine impedir que alguém entre num prédio bloqueando a rua inteira. O problema é que essa rua também leva a hospitais, escolas e casas, então, ao fechar tudo, você atrapalha diversas pessoas que precisam passar por ali para serviços essenciais. E, no fim das contas, quem estiver realmente decidido ainda vai achar outro jeito de entrar, mesmo com a rua bloqueada. Isso é semelhante ao que ocorre quando governos tentam impedir o acesso a sites específicos ou a conteúdos on-line, desligando partes da Internet por meio de métodos de bloqueio do Sistema de Nomes de Domínio (DNS) ou de endereços de Protocolo de Internet (IP). Embora essa abordagem possa parecer rápida e simples, ela frequentemente causa mais impacto do que o desejado, prejudicando outros serviços e deixando de resolver o problema central.

O bloqueio baseado em IP e DNS surgiu como o método mais comumente proposto devido à sua aparente simplicidade e facilidade de implementação, e os governos ao redor do mundo estão cada vez mais instruindo os Provedores de Serviços de Internet (ISPs) e resolvedores de DNS a bloquear o acesso a conteúdos da Internet que consideram ilegais ou questionáveis, como jogos de azar não autorizados, material de abuso infantil, violação de direitos autorais e ameaças à segurança nacional.1 . No entanto, esses métodos muitas vezes não conseguem abordar de forma eficaz as causas fundamentais dos problemas visados e podem provocar interrupções técnicas significativas e danos sociais.

Embora o bloqueio de conteúdo possa parecer uma solução rápida para impedir o acesso a material ilegal, muitas vezes é ineficaz e frequentemente provoca o bloqueio de serviços legítimos, impactando tanto usuários quanto empresas. Além disso, o bloqueio de DNS e IP não remove o conteúdo da Internet, tornando o material ainda acessível para pessoas determinadas a desviar do bloqueio. Tentativas de contornar o bloqueio podem colocar em risco a privacidade, a segurança e a proteção dos usuários.

[1] i2Coalition. *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet*, 03 de junho de 2025. Disponível em: https://i2coalition.com/i2coalition-launches-dns-at-risk-report-and-website-to-spotlight-rising-global-internet-infrastructure-abuse/

A Internet Society apresentou uma análise técnica dos métodos de bloqueio mais comuns, destacando suas limitações e seus potenciais riscos. A análise indica que ambas as técnicas podem ser contornadas facilmente, são imprecisas e propensas a causar danos colaterais. A Internet Society incentiva que os legisladores priorizem soluções que combatam o conteúdo prejudicial em sua origem, em vez de recorrerem a medidas técnicas rígidas que podem gerar externalidades negativas para a natureza aberta e global da Internet.

O bloqueio de DNS e IP, por sua própria concepção, interfere nos mecanismos básicos que permitem aos usuários encontrar e acessar informações na Internet. A implementação de bloqueio baseado em DNS e IP envolve mais do que apenas a execução técnica. Essas abordagens impactam o funcionamento da Internet em um nível fundamental, e seu uso pode acarretar consequências significativas operacionais, jurídicas e sociais. Esta seção apresenta fatores críticos que devem orientar qualquer consideração de políticas sobre bloqueio de conteúdo.

O bloqueio baseado em IP impede o acesso a conteúdos ao bloquear o estabelecimento de conexões TCP/IP com endereços IP específicos, interrompendo efetivamente a comunicação com servidores-alvo. **Já o bloqueio baseado em DNS** manipula o Sistema de Nomes de Domínio, retornando respostas falsas ou enganosas quando um usuário tenta acessar um domínio bloqueado, fazendo o conteúdo parecer inacessível.

Ambas as abordagens, geralmente, são estabelecidas em nível nacional e implementadas nas redes dos Provedores de Serviços de Internet (ISPs). Elas são preferidas em círculos de formulação de políticas por sua aparente simplicidade e escalabilidade. No entanto, essas técnicas podem carecer de precisão e são facilmente contornadas por usuários por meio de VPNs (redes privadas virtuais) ou da troca de resolvedores de DNS, enquanto provedores de conteúdo podem simplesmente alterar a infraestrutura na qual o conteúdo é hospedado.

O que define o problema, em última análise, é a disparidade entre os resultados de política pretendidos e os efeitos técnicos reais. Esses métodos não removem o conteúdo da Internet, nem tratam sua origem. Em vez disso, eles impõem barreiras de acesso que são pouco confiáveis e propensas a causar danos colaterais. Essa incompatibilidade entre objetivos de política e realidades técnicas mostra a necessidade de respostas mais realistas, eficazes e menos disruptivas.

Desafios

A implementação de bloqueio baseado em DNS e IP envolve uma série de desafios técnicos, sociais, econômicos e políticos complexos. No nível técnico, essas medidas são instrumentos intrinsecamente

rígidos que têm dificuldade em distinguir entre conteúdo ilegal e legítimo quando ambos estão hospedados no mesmo endereço IP ou resolvidos no mesmo domínio. Como resultado, serviços legais são frequentemente pegos no fogo cruzado, levando a bloqueios excessivos e ao risco de interrupção no acesso a informações e plataformas essenciais.

Imagine um servidor hospedando tanto um site de streaming pirata quanto um pequeno site de comércio eletrônico usando o mesmo endereço IP. Uma ordem para bloquear esse IP também bloqueará o acesso ao site de comércio eletrônico, prejudicando operações comerciais legítimas, mesmo que o site não tenha envolvimento com pirataria[2]. Isso demonstra como o bloqueio em nível de IP pode causar interrupções abrangentes em serviços, muito além da intenção original.

Em uma tentativa de recuperar o acesso, os usuários podem recorrer a ferramentas como VPNs ou diferentes resolvedores de DNS. O perigo é que, ao tentarem contornar o bloqueio de conteúdo, esses usuários podem escolher, inadvertidamente, VPNs ou resolvedores de DNS que prometem acesso, mas oferecem menor proteção de segurança e privacidade. Como resultado, a experiência desses usuários na Internet pode ser menos segura. Empresas legítimas podem ser forçadas a mover seus serviços para um endereço IP ou domínio não bloqueado, ou para outro provedor de hospedagem.

Entre 2024 e 2025, a Itália implementou seu sistema "Piracy Shield", um esquema antipirataria agressivo que exige que ISPs, serviços de DNS e provedores de VPN bloqueiem domínios e IPs ligados a streaming esportivo ilegal em até 30 minutos após solicitação dos detentores de direitos3. No entanto, essa política bloqueou repetidamente serviços legítimos, incluindo domínios do Google, sites hospedados pela Cloudflare e o Google Drive, causando ampla interrupção para negócios, usuários comuns da Internet e serviços4 em nuvem.

O bloqueio de domínios em nível de resolvedores de DNS públicos pode ter consequências não intencionais que vão além do controle de conteúdo, afetando diretamente a segurança on-line dos usuários nos países onde esses serviços operam. Por exemplo, resolvedores recursivos públicos como o Quad9[5] desempenham um papel fundamental na proteção dos usuários contra malware, phishing e outras ameaças cibernéticas, filtrando domínios prejudiciais com base em feeds globais de inteligência sobre ameaças.

Quando os governos exigem que esses resolvedores direcionem recursos técnicos e operacionais para implementar bloqueios específicos de conteúdo, isso pode minar suas funções de segurança principais. Isso não apenas enfraquece a proteção para indivíduos e empresas, mas também pode diminuir a

[2] The i2Coalition, *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet*, maio de 2025, p. 8, disponível em: https://i2coalition.com/wp-content/uploads/2025/05/DNS-at-Risk-How-Network-Blocking-and-Fragmentation-Undermine-the-Global-Internet.pdf.

[3] TechRadar, *Italy's Piracy Shield may be breaching EU law...*, 10 de julho de 2025

[4] DediRock, *Report Highlights Risks of Government DNS Blocking*, junho de 2025

[5] Quad9. *About Quad9*. Disponível em: https://quad9.net/about

resiliência cibernética de um país ao remover ou comprometer uma camada confiável da infraestrutura. O risco é que, ao buscar a aplicação de bloqueios em sites específicos, as autoridades inadvertidamente acabam enfraquecendo um serviço defensivo que beneficia milhões de usuários, deixando-os mais vulneráveis a fraudes on-line, roubo de identidade e ataques à rede.

A partir de uma **perspectiva econômica,** medidas de bloqueio baseado em DNS e IP podem impor custos substanciais a Provedores de Serviços de Internet e operadores de rede. Esses custos englobam despesas operacionais para implementar e manter sistemas de bloqueio, perdas de receita para plataformas on-line e negócios afetados pelo excesso de bloqueios, e ineficiências econômicas mais amplas causadas pela redução de confiança e confiabilidade na infraestrutura da Internet[6].

Princípios orientadores e recomendações

A Internet Society acredita que a maneira mais adequada de combater conteúdo e atividades ilegais na Internet é enfrentá-los em sua origem. Usar DNS ou endereços IP para bloquear acesso a conteúdo on-line provavelmente é ineficaz e propenso a causar danos colaterais, afetando usuários inocentes da Internet. Por essas razões, e devido aos desafios mencionados acima, desaconselhamos o bloqueio de conteúdo. No entanto, essas técnicas ainda são usadas. Reconhecendo essa realidade, sugerimos duas estratégias principais para os legisladores preocupados com conteúdo ilegal na Internet:

- **Enfrentar o problema na origem:** a abordagem menos danosa para a Internet é "atacar" o conteúdo e as atividades ilegais em sua origem. A remoção do conteúdo ilegal de sua origem e a aplicação de ações de fiscalização no ponto de origem evita os efeitos negativos do bloqueio e são mais eficazes para a remoção de conteúdo ilegal. A cooperação entre jurisdições e partes interessadas é um pré-requisito para o sucesso, já que o conteúdo ilegal on-line ultrapassa fronteiras e leis nacionais.
- **Priorizar e usar abordagens alternativas, por exemplo:**
    - A cooperação eficaz entre provedores de serviço, forças policiais e autoridades nacionais pode oferecer meios adicionais para ajudar vítimas de conteúdo ilegal e promover ações de aplicação da lei.
    - A criação de um ambiente de confiança, no qual os usuários recebam informações sobre o que é legal e o que não é, pode estimular o autopoliciamento. Em alguns casos (por exemplo, controle parental), capacitar o usuário a utilizar filtros em seus próprios dispositivos, com seu consentimento, pode ser eficaz e menos prejudicial para a Internet.

[6] Analysys Mason, *The economic cost of network blocking*, report for Cloudflare, 28 de julho de 2025. Disponível em: https://www.analysysmason.com/consulting/reports/network-blocking-economic-impact-jul25/

E oferecemos as seguintes diretrizes específicas para reduzir o impacto negativo do bloqueio de conteúdo:

- **Esgote todas as opções que não sejam de bloqueio:** em primeiro lugar, esgote todas as opções práticas para tratar o conteúdo na origem ou por outros meios alternativos ao bloqueio. O bloqueio de conteúdo não deve ser adotado apenas por ser mais fácil. Ele deve ser necessário e proporcional.
- **Seja transparente:** deve haver transparência sobre o bloqueio, bem como sobre o objetivo e as políticas subjacentes de bloqueio de conteúdo. Os governos devem garantir que os usuários afetados possam levantar preocupações sobre os impactos negativos em seus direitos, interesses e oportunidades.
- **Empodere os usuários**: os usuários devem poder filtrar conteúdo ilegal ou indesejado em seus próprios dispositivos ou redes, garantido o acesso a ferramentas de segurança on-line e treinamento em habilidades digitais.
- **Restrinja o escopo:** bloqueie o conteúdo de forma mais local possível para minimizar o impacto global.
- **Envolva as partes interessadas:** o desenvolvimento e a implementação de políticas sobre conteúdo on-line devem envolver um amplo conjunto de partes interessadas, incluindo especialistas em tecnologia, economia, direitos do consumidor e outros, para garantir que medidas apropriadas sejam tomadas para minimizar os efeitos adversos das políticas destinadas a tratar desse conteúdo.
- **Siga o devido processo legal:** qualquer ordem de bloqueio de conteúdo ilegal deve ter respaldo legal, ser revisada de forma independente e direcionada de maneira específica para alcançar um objetivo legítimo. Deve-se priorizar o meio menos restritivo disponível para lidar com atividades ilegais. Prestadores de serviços de Internet ou outros intermediários da Internet não devem substituir os agentes oficiais de aplicação da lei: eles não devem ser obrigados a determinar quando a conduta ou o conteúdo é ilegal.
- **Tome medidas temporárias:** quaisquer medidas de bloqueio devem ser temporárias. Elas devem ser removidas assim que deixar de existir o motivo do bloqueio. É muito comum que o conteúdo ilegal seja movido para evitar as medidas de bloqueio, contudo, as medidas frequentemente permanecem em vigor muito tempo depois de o conteúdo ter sido movido.

A oposição da Internet Society ao bloqueio baseado em DNS e IP baseia-se em como essas técnicas comprometem as propriedades fundamentais da Internet, conforme definidas no **Internet Way of Networking (IWN).** Esses métodos de bloqueio prejudicam a arquitetura técnica que torna a Internet aberta, globalmente acessível e resiliente.

A Internet Society desenvolveu uma descrição técnica desses princípios fundamentais. Chamamos isso de "The Internet Way of Networking", uma estrutura que descreve o que torna a Internet única em

relação a outras redes. Desenvolvemos o "Kit de Ferramentas de Avaliação do Impacto da Internet"[7] para ajudar a nossa comunidade de especialistas técnicos, de políticas e outros a usar essa estrutura. Ele pode identificar onde políticas, decisões comerciais, regulamentações ou tendências podem impactar a base única da Internet, ou quais são as melhores práticas para preservá-la.

[7] Internet Society. *Internet Impact Assessment Toolkit*, 2020. Disponível em: https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/